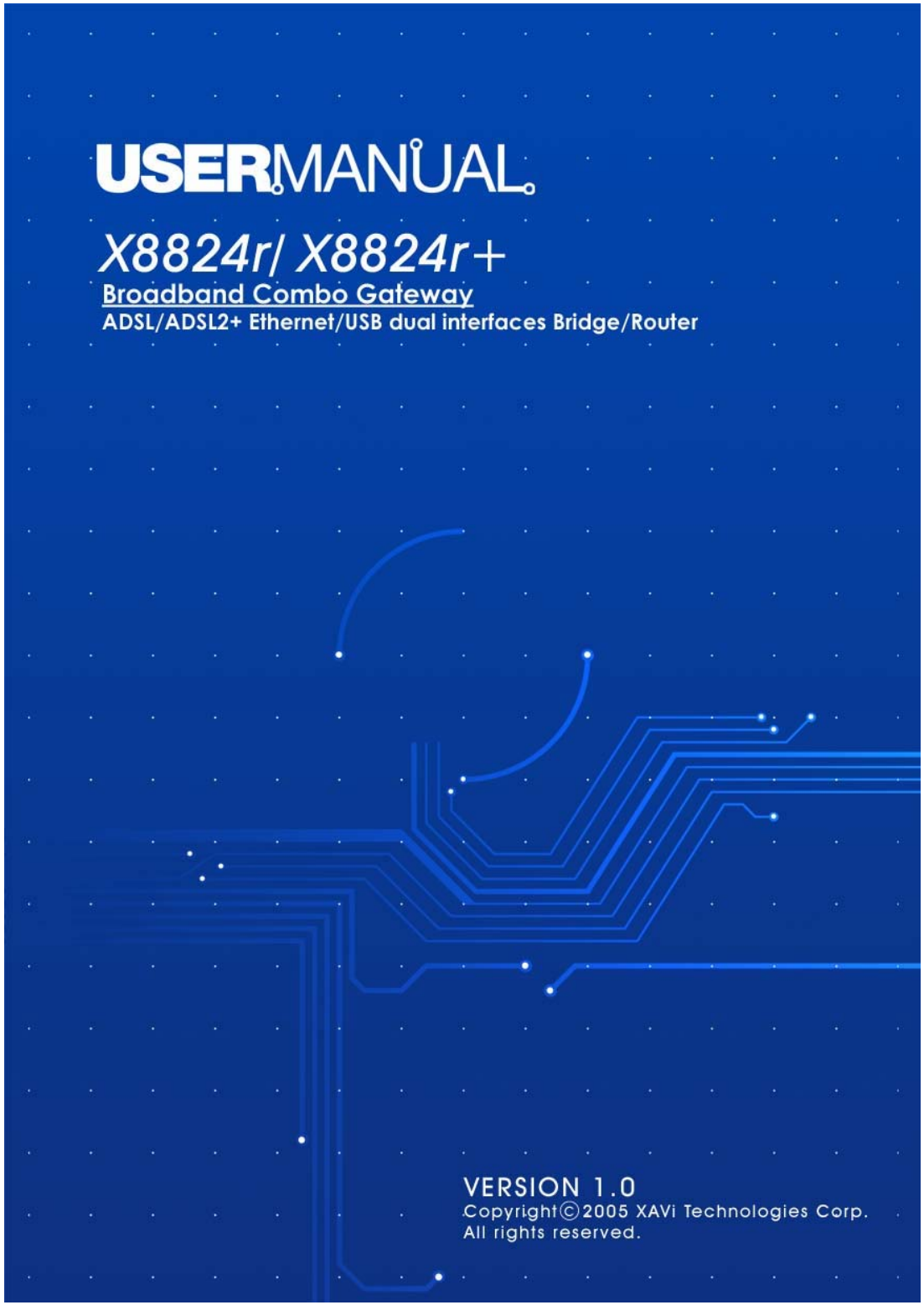


Tel: +886-2-2995-7953
9F, No. 129, Hsing Te Road, Sanchung City,
Taipei Hsien 241,
Taiwan

Copyright © 2003, XAVi Technologies Corporation

Information in this manual is subject to change without notice. No part of this manual may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying or scanning, for any purpose, without the written permission of XAVi Technologies Corporation.

XAVi Technologies Corporation provides this documentation without warranty of any kind, implied or expressed, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose.

Table of Contents

Chapter 1 – Getting Started

1. OVERVIEW 7
2. FEATURES 8
4. APPEARANCE 10
5. HARDWARE INSTALLATION 12
6. MANAGEMENT 13
7. DEFAULT VALUES 14
8. SOFTWARE UPGRADE 15

Chapter 2 – Web Interface Management

1. OVERVIEW 16
2. PREPARATION 16
3. LOGIN 17
4. HOME 18
5. LAN 20
5.1 LAN CONFIG 20
5.2 DHCP MODE 23
5.3 DHCP SERVER 24
5.4 DHCP RELAY 26
6. WAN 27
6.1 DSL 27
6.2 ATM VC 29
6.3 POINT TO POINT PROTOCOL (PPP) 31

6.4 ETHERNET OVER ATM (EOA) 35
6.5 IP OVER ATM (IPOA) 38
7. BRIDGING 41
7.1 BRIDGING 41
8. ROUTING 42
8.1 IP ROUTE 42
9. SERVICES 43
9.1 NAT 44
9.2 RIP 47
9.3 FIREWALL 49
9.4 IP FILTER 51
9.5 DOMAIN NAME SERVICE (DNS) 54
9.6 BLOCKED PROTOCOLS 56
10. ADMIN 61
10.1 USER CONFIG 61
10.2 COMMIT & REBOOT 63
10.3 LOCAL IMAGE UPGRADE 64
10.4 REMOTE IMAGE UPGRADE 65
10.5 ALARM 65
10.6 DIAGNOSTICS 66
10.7 PORT SETTINGS 66
10.8 SYSTEM LOG 67
10.9 BACK/ RESTORE CONFIG 68
10.10 MANAGEMENT CONTROL 69

Chapter 3 – Quick Protocol Setup

1. OVERVIEW 73
2. RFC 1483 BRIDGE 74
3. PPPOE ROUTE CONFIGURATION 78
4. RFC 1483 + NAT 82
5. PPPOA ROUTE CONFIGURATION 86
6. IPOA ROUTE CONFIGURATION 90
7. DHCP CONFIGURATION 92
8. NAT CONFIGURATION 94

APPENDIX A – SPECIFICATIONS **96**
APPENDIX B – WARRANTIES **97**
APPENDIX C – REGULATIONS **100**

CONTACT INFORMATION **102**

Revision Marks

Revision	Date	Notes
V 1.0	July 31, 2005	Software Version: 3.C52XAT1.8824/2.5.050505c

Chapter 1

Getting Started

1. Overview

X8824r and **X8824r+** are ADSL/ADSL2+ series of customer premise equipments that provide high-speed asymmetrical data transmission on a single twisted copper pair. The DSL line interface supports various ADSL standards, up to ADSL2+ with **X8824r+**. At the DTE side these CPEs provide one 10/100 Ethernet interface and one USB port for easy connection to user's PC or LAN environment. With built-in IP routing, NAPT and firewall, these units serve as the gateway to the Internet world. **X8824r** and **X8824r+** deliver broadband access for enterprises, telecommuters, home, and remote office workers with high-speed data transfer requirements.

2. Features

- Compliant with ITU-T G.992.1 (G.dmt), G.992.2 (G.lite) and ANSI T1.413 Issue 2
- X8824r+ is additionally compliant with ITU-T G.992.3 (G.dmt.bis / ADSL2), G.992.5 (ADSL2+) and provides up to 24 Mbps downstream rate
- Compatible and interoperable with major Central Office side ADSL DSLAM or Multi-service Access System
- One 10/100 Base-TX Ethernet port and one USB 1.1 device port for PC / LAN connection
- RFC2684 / 1483 to bridge or route traffic over ATM over ADSL
- Support Networking protocols such as PPP, IP routing, NAPT, DHCP server / relay / client
- Can work either in Bridge or Router mode
- Support local and remote configuration and management through Web, Telnet or SNMP
- Simple firmware upgrade via TFTP, FTP or HTTP

3. Packaging

This package consists of the following items:

X8824r ADSL device unit

RJ-45 Cable

RJ-11 Cable

AC Adapter

User's Manual CD

4. Appearance

Front Panel

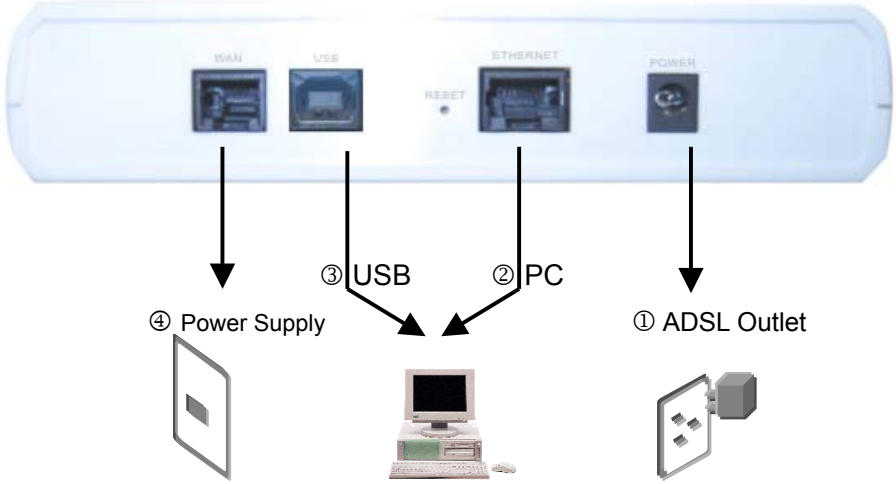
	Label	LED Status	Color	Description
①	PWR	ON	Green	Power supply is connected.
②	WAN	Blinking	Green	Training with DSLAM.
		ON	Green	ADSL link is ready.
③	PPP	ON	Green	PPP sync up
		Blinking	Green	Data transmitting
④	LAN	ON	Green	Ethernet transmitting
⑤	USB	ON	Green	USB port is connected

Rear Panel

	Label	Description
①	WAN	RJ-45 port; connect to a PC or LAN.
②	USB	USB port; connect to PC or LAN
③	RESET	Reset the modem back to factory settings by holding down on this button.
④	ETHERNET	RJ-11 or RJ-45 port; connect to the ADSL outlet. ***X8824r*** *uses RJ-11 Cable.*
⑤	PWR	Power jack; connect to a power adapter.

5. Hardware Installation

1. Connect one end of the ADSL cable to the WAN port of ***X8824r*** and the other end to the ADSL wall outlet.
2. Use a RJ-45 cable to connect one end to the Ethernet port of ***X8824r,*** and the other end to the LAN or a PC with an Ethernet adapter installed.
3. Use a USB cable to connect one end to the USB port of X8824r, and the other end to a PC with a USB port.
4. Plug in the AC adapter to the AC power socket, and then connect the DC jack to the PWR inlet of ***X8824r.***



Note: Be sure to use a RJ-45 crossover cable while connecting to a hub.

6. Management

The device supports simple, flexible, and easy-to-operate methods for management purposes. ***X8824r*** can be managed via the following paths:

- ✓ **Local Ethernet Port (Telnet)** – connect the Ethernet port to your local area network or directly to a PC. "*Telnet*" ***X8824r*** from any workstation in the LAN. The default local Ethernet IP address is "**192.168.1.1**".
- ✓ **Local Ethernet Port (Web Browser)** – connect the Ethernet port to your local area network or directly to a PC. Launch your web browser and enter default local Ethernet IP address "**192.168.1.1**" into the address bar.
- ✓ **ADSL Port from Remote Site** – while the ADSL connection is in service, you may remotely "*Telnet*" ***X8824r*** from a workstation connected to the CO equipment.

Note: As operating an ADSL device requires technical know-how and experience. It is recommended that only qualified technical staffs manage the device. Therefore, a password authentication is required when you enter the web interface. To obtain the password, see the *Default Values* section.

7. Default Values

This device is pre-configured with the following parameters; you may also re-load the default parameters by rebooting the router into the Default configuration from the web browser.

Default Mode: Bridge	**Login Name: admin**
	Password: **admin**
Bridge Mode Setting	**WAN and ADSL**
Ethernet (local) IP: 192.168.1.1	Local Line Code: Auto
Subnet Mask: 255.255.255.0	Trellis Mode: Enable
Full Duplex: Auto	FDM Mode: EC
Protocol: RFC1483, Bridge Mode	Coding Gain: Auto
VPI/VCI: 8/35	Transmit Power Attenuation: 0dB
Class (QoS): UBR	
Spanning Tree: Disable	
Packet Filter: Any	
Router Mode Setting	**DHCP Server:** Disable
Ethernet (local) IP: 192.168.1.1	**DNS Relay:** Disable
Subnet Mask: 255.255.255.0	

Note: The User Name and Password are case-sensitive.

8. Software Upgrade

You may easily upgrade the embedded software by obtaining the compressed upgrade kit from the service provider then following the steps:

Click on the **Local Image Upgrade** link to upgrade the software on the modem.
You may easily upgrade the embedded software by obtaining the compressed upgrade kit from the service provider and then following the steps:

a. Click on the **Browse** button to select the upgrade file.
b. Click on the **Upload** button to upload the file into the modem
c. This process may last as long as 60 seconds.

Note: Strictly maintain stable power to the device while upgrading its software. If the power fails during the upgrading process, contents in the memory could be destroyed, and the system may hang. In such a case, you must call the dealer or system integrator for repairs.

Chapter 2

Web Interface Management

1. Overview

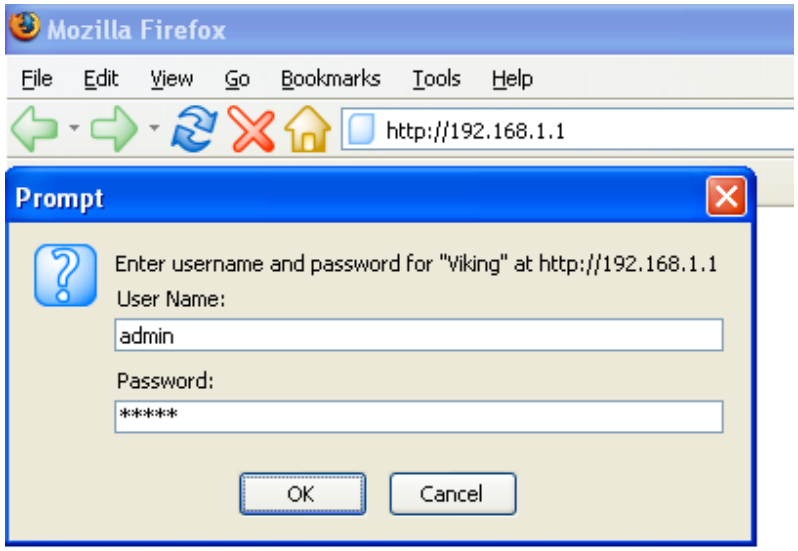
The Web management is provided in order to manage the ADSL device as easily as possible. It provides a very user-friendly configuration and graphical interface through a Web based platform. You can configure a bridge or a router, as you feel appropriate. In the section below, each configuration item is described in detail.

2. Preparation

1) Please refer the hardware installation procedure to install modem.
2) You should configure the PC to the same IP subnet as the modem.
   For example: The modem: 192.168.1.1
   Your PC: 192.168.1.**x**
3) Let your PC access the modem, and make sure that the PING function is working properly. The default IP address of this modem could be found in the default settings section.
4) Open the Web browser (Internet explorer or Netscape), enter the default IP address "**192.168.1.1**" for the website address to access the web management page.
5) The **Login** dialog box will pop up first.

3. Login

- The window **Enter Network Password** will pop up while starting the configuration. With the window open, type **admin** for both the **Username** and the **Password**.



- After you log into the web interface, you will notice that it is divided into seven different sections, or tabs. From this point on, each tab is described in detail along with instructions for configuration. The seven tabs are: **Home, LAN, WAN, Bridging, Routing, Services,** and **Admin.**

4. HOME

- After logging in, the first tab that will be displayed is the **Home** tab. Under this tab, the **System View** page is displayed. This page displays a summary of the interfaces and their settings.

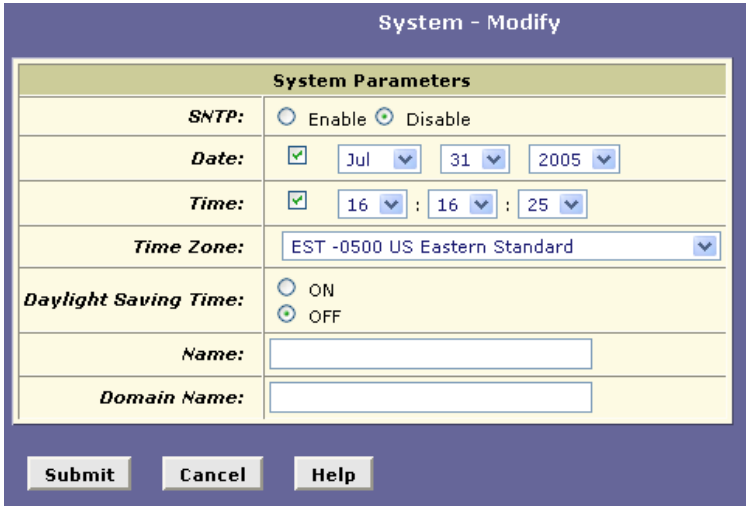
Home LAN WAN Bridging Routing Services Admin
Home | System Mode | Quick Configuration
System View
Use this page to get the summary on the existing configuration of your device.
Device
Model: Vulcan
H/W Version: 810100
S/W Version: 3.C52XAT1.8824/2.5.050505c
Serial Number: 123456789abcdx
Mode: Routing And Bridging
Up Time: 0:5:34
Time: Thu Jan 01 00:05:34 1970
Time Zone: GMT
Daylight Saving Time: OFF
Name:
Domain Name:
DSL
Operational Status: Showtime/Data
Last State: 0x19
DSL Version: E.21.1.16
Annex Type: ADSL2
Standard: ADSL2+
Connected Standard: G.dmt
Data Boost: -
Profile Main
Up Speed 1024 Kbps Latency Interleaved
Down Speed 8064 Kbps Latency Interleaved
WAN Interfaces
Interface Encapsulation IP Address Mask Gateway Lower Interface VPI/VCI Status
eoa-0 Bridged 0.0.0.0 0.0.0.0 0.0.0.0 aal5-0 8/35
LAN Interface
Interface Mac Address IP Address Mask Lower Interface Speed Duplex Status
eth-0 00:85:A0:01:01:00 192.168.1.1 255.255.255.0 - 100BT Full
usb-0 - 192.168.1.2 255.255.255.0 - - -
Services Summary
Interface NAT IP Filter RIP DHCP Relay DHCP Client DHCP Server IGMP
eth-0 inside
eoa-0 outside
usb-0 inside
Modify Refresh Help

- This page is divided into five sections. The table below describes each section.

Section Name	Description
Device	Displays model name, hardware/software version, device mode, uptime, current time, time zone, daylight savings time, and domain name.
DSL	Displays operation status, last state, DSL version, and DSL standard.

WAN Interfaces	Displays the WAN interface name, encapsulation type, IP address, subnet mask, lower interface, VPI/VCI values, and operational status.
LAN Interface	Displays the LAN interface name, MAC address, IP address, subnet mask, lower interface, transmission speed, duplex type and operational status.
Services Summary	Displays the interface name, and enabled/disabled features, such as: NAT, IP filter, RIP, DHCP relay, DHCP client, DHCP server, and IGMP. A green check mark (✓) indicates that the service has been enabled. A red cross (✗) indicates the service has been disabled.

- To add, change, or remove any of the interface settings, click on the interface name.
- Click on the **Modify** button to set the device date, time, time zone, and other related settings. Click on the **Submit** button when completed.



- **SNTP:** Select **Enable** if you would like the time to be assigned by an SNTP server. By selecting this option you will not be required to enter the time, date, or time zone. However, you must enter the domain name, which is the SNTP address.
- **Date:** Enable this check box and select the date from the drop-down list.
- **Time:** Enable this check box and select the time from the drop-down list.
- **Daylight Saving Time:** Select **ON** or **OFF** as necessary.
- **Name**: Enter the name of the SNTP server.
- **Domain Name**: Enter the domain name or IP address of the SNTP server.
- Click on the **Submit** button when completed and make sure to **Commit & Reboot**.

5. LAN

Click on the **LAN** tab to view its sub-menu's and configure the LAN settings. The four sub-menu's are: LAN Config, DHCP Mode, DHCP Server, and DHCP Relay. Each sub-menu is described below.

5.1 LAN Config

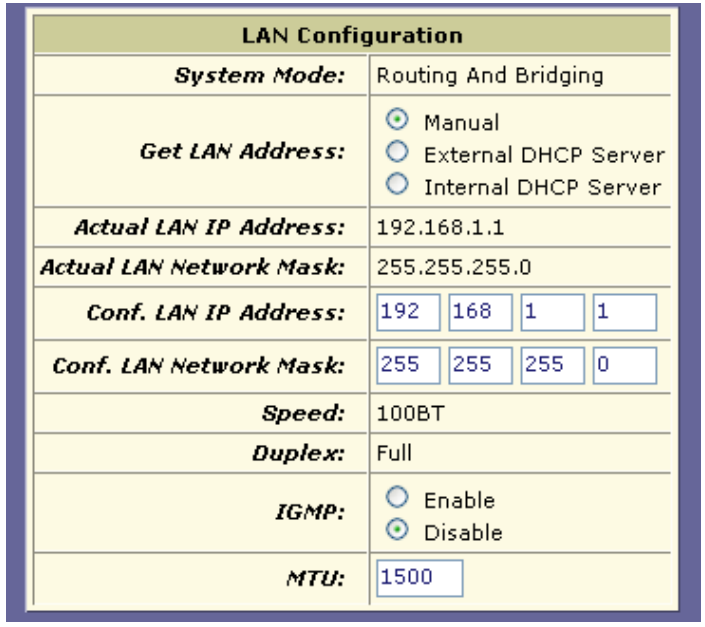
Click on the **LAN Config** link to change the LAN IP address/ subnet mask of the Ethernet and USB interface, decide where the LAN is getting its IP address from, and enable or disable IGMP.

If you are using the ADSL/Ethernet router with multiple PCs on your LAN, you must connect the LAN via an Ethernet hub connected to the device's LAN port. If you are using a single PC with the ADSL/Ethernet router, you have two connection options:

You can connect the PC directly to the LAN port using a cross-over Ethernet cable.

If the PC is USB-enabled, you can connect it directly to the device's USB port. Only one computer can be connected in this manner.
You can also use the USB and Ethernet interfaces simultaneously, connecting your LAN to the Ethernet port and a standalone PC to the USB port.

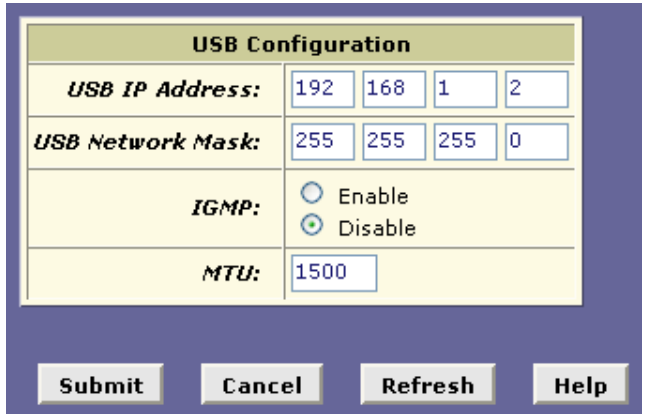
Follow the steps below in order to set up the LAN.



- **Get LAN Address:** Select **Manual** if you would like to enter your own IP address. Select **External DHCP Server** if a DHCP server other than this device assigns the IP addresses. Select **Internal DHCP Server** if you would like this device to assign the IP addresses.
- **LAN IP Address:** Enter the LAN IP address into these text boxes. This is the IP address for the Ethernet port.
- **LAN Network Mask:** Enter the subnet mask of the LAN IP address into these text boxes. This is the subnet mask for the Ethernet port.
- **IGMP:** ındicates whether this interface is enabled with the Internet Group Management Protocol. When enabled, the

ADSL/Ethernet router collects and consolidates requests from the LAN PCs to receive IGMP messages from external computers. The interface also forwards IGMP messages it receives on its WAN interface to the appropriate hosts. The WAN interface must also be enabled for the IGMP protocol Depending on your ISP's settings, choose to enable or disable IGMP.

- **MTU:** The Maximum Transmission Unit specifies the size in bytes of the largest Ethernet packet that the interface will accept. Packets larger than this size will be dropped.
- Click on the **Submit** button when completed and make sure to **Commit & Reboot**.



- **USB IP Address:** Enter the LAN IP address into these text boxes. This is the IP address for the USB port.
- **USB Network Mask:** Enter the subnet mask of the LAN IP address into these text boxes. This is the subnet mask for the USB port.
- **IGMP:** ındicates whether this interface is enabled with the Internet Group Management Protocol. When enabled, the ADSL/Ethernet router collects and consolidates requests from the LAN PCs to receive IGMP messages from external computers. The interface also forwards IGMP messages it receives on its WAN interface to the appropriate hosts. The WAN interface must also be enabled for the IGMP protocol Depending on your ISP's settings, choose to enable or disable IGMP.

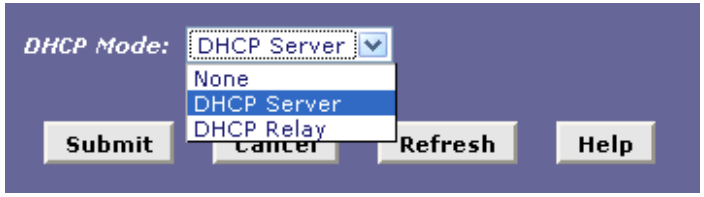
- **MTU:** The Maximum Transmission Unit specifies the size in bytes of the largest Ethernet packet that the interface will accept. Packets larger than this size will be dropped.
- Click on the **Submit** button when completed and make sure to **Commit & Reboot**.

5.2 DHCP Mode

Click on the **DHCP Mode** link to select a DHCP setting. From the drop down list, select **DHCP Server, DHCP Relay,** or **None** and click on the **Submit** button.

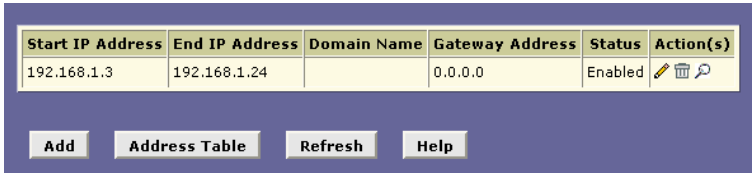
DHCP is a protocol that enables network administrators to centrally manage the assignment and distribution of IP information to computers on a network.

When you enable DHCP on a network, you allow a device - such as your ADSL/Ethernet router or a router located with your ISP - to assign temporary IP addresses to your computers whenever they connect to your network. The assigning device is called a DHCP server, and the receiving device is a DHCP client.

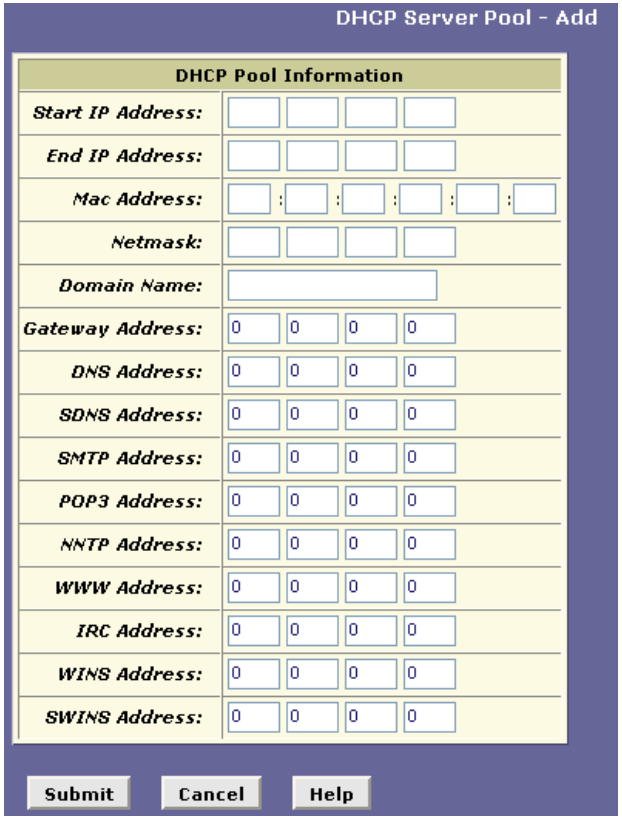


5.3 DHCP Server

Click on the **DHCP Server** link to view the DHCP Server settings. The table displays the DHCP server settings, this includes: start IP, end IP, domain name, gateway address, and status.



Click on the **Add** button to enable a DHCP server and fill in the IP information based on your ISP settings.



An IP address pool typically includes a range private addresses that you define. LAN administrators often define private IP addresses for use only on their networks. You can also use DHCP server pools to distribute multiple public IP addresses, if, for example, these are to be shared among a larger set of LAN computers.

You can create up to two DHCP server address pools. You can define a single pool with addresses that can be assigned to your LAN PCs (connected via the Ethernet port) and to a USB-connected computer, as long you have assigned to the USB and Ethernet interfaces static IP addresses that place them in the same subnet.

- **Start/End IP Addresses:** Specify the lowest and highest addresses in the pool, up to a maximum range of 254 addresses.
- **Mac Address:** A MAC address is a manufacturer-assigned hardware ID that is unique for each device on a network. Use this field only if you want to assign a specific IP address to a specific computer (that is, you are creating an exception to the dynamic assignment of addresses). The IP address you specify will be assigned to the computer that corresponds to this MAC address. If you type a MAC address here, you must have specified the same IP address in both the Start IP Address and End IP Address fields.
- **Net Mask:** Specifies which portion of each IP addresses in this range refers to the network and which portion refers to the host (computer). You can use the net mask to distinguish which pool of addresses should be distributed to a particular subset of computers on your LAN (call a subnet).
- **Domain Name:** A user-friendly name that refers to the subnet that includes the addresses in this pool.
- **Gateway Address:** The address of the default gateway for computers that receive IP addresses from this pool. If no value is specified, then the appropriate LAN (eth-0) or USB (usb-0) port address on the device will be distributed to each PC as its gateway address, depending on how each is connected. See Configuring IP Routes for an explanation of gateway addresses.

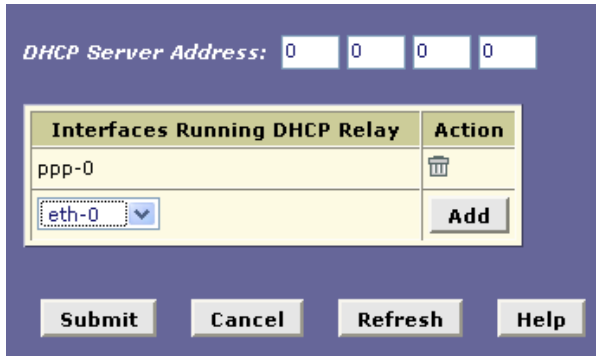
- **DNS/SDNS:** The IP address of the Domain Name System server to be used by computers that receive IP addresses from this pool. The DNS translates common Internet names that you type into your web browser into their equivalent numeric IP addresses. Typically, this server is located with your ISP.
- **SMTP...SWINS (optional):** The IP addresses of devices that perform various services for computers that receive IP addresses from this pool (such as the SMTP, or Simple Mail Transfer Protocol, server which handles e-mail traffic). Contact your ISP for these addresses.
- Click on the **Submit** button when completed and make sure to **Commit & Reboot**.

5.4 DHCP Relay

Click on the **DHCP Relay** link to view the DHCP Relay settings.

Some ISPs perform the DHCP server function for their customers' home/small office networks. In this case, you can configure the device as a DHCP relay agent. When a computer on your network requests Internet access, the ADSL/Ethernet router connects your ISP to obtain an IP address and other information, and then forwards that information to the computer.

Fill in the DHCP server IP address in the text boxes and select an interface name from the dorp down list, then click on the **Add** button.



6. WAN

Click on the **WAN** tab to view its sub-menu's and configure the WAN settings. The five sub-menu's are: DSL, ATM VC, PPP, EOA, and IPOA. Each sub-menu is described below.

6.1 DSL

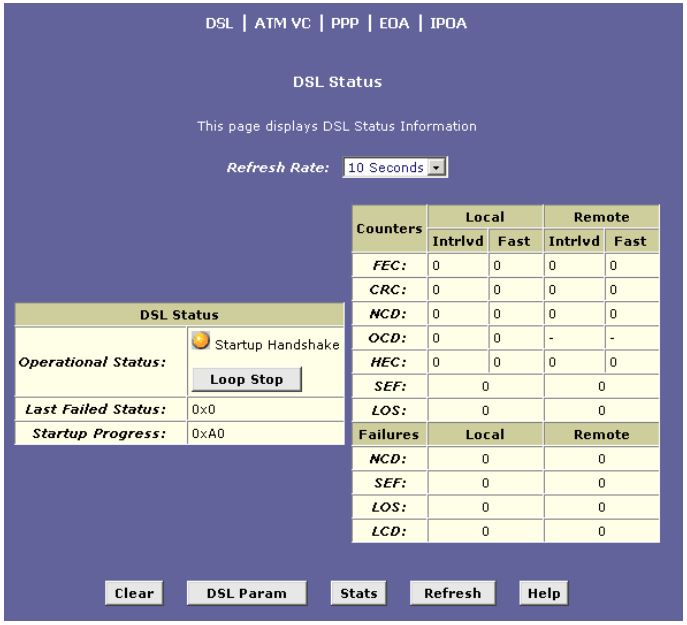
The **DSL** Status page displays current information on the DSL line performance. The page refreshes according to the setting in the Refresh Rate drop-down list, which you can configure.

In the DSL Status table, the Operational Status setting displays a red, orange, or green ball to indicate that the DSL line is idle, starting up, or up-and-running, respectively. You can click Loop Stop to end the DSL connection. To restart the connection, you can click Loop Start.

Although you generally will not need to view the remaining parameters, they may be helpful when troubleshooting connection or performance problems with your ISP.

Click on the **DSL** link to view the DSL status. Click on the **DSL Param** button to view the DSL parameters and the **Stats** button to view the DSL statistics. Both the **DSL Parameters** and **DSL Statistics** are described below.

Click on the **Clear** button to clear and refresh the DSL status. You may also change the page refresh rate by selecting a different time period from the **Refresh Rate** drop down list.

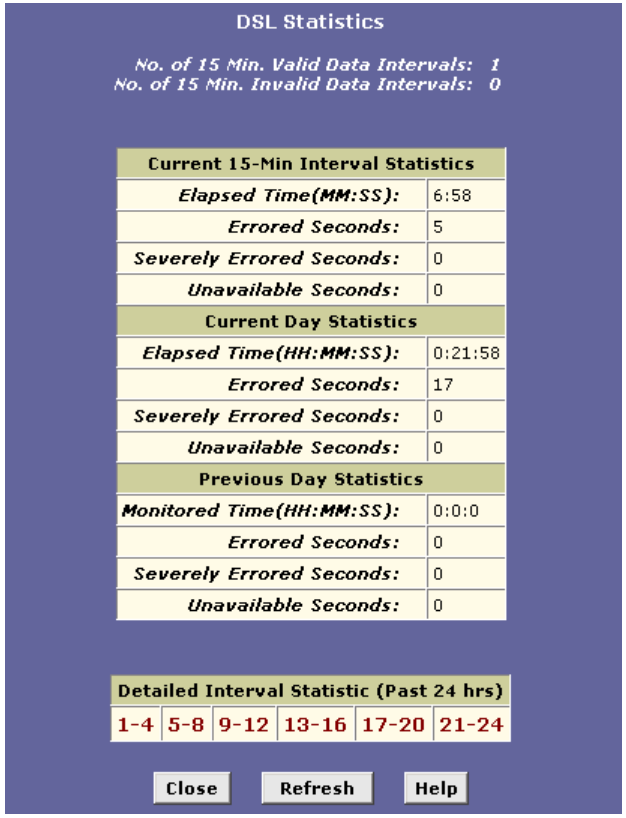


a) DSL Parameters

Click on the **DSL Param** button to view the DSL parameters. Another window will then display the DSL parameters, which may be different due to the type and speed of the network. Click on the **Close** button to close the window, or click on the **Refresh** button to refresh the status.

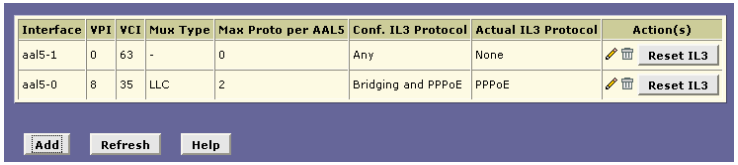
b) DSL Stats

Click on the **Stats** button to view the DSL status. Another window will then display the DSL status, which may be different due to the type and speed of the network. Click on the **Close** button to close the window, or click on the **Refresh** button to refresh the status.



6.2 ATM VC

Click on the **ATM VC** link to view the ATM VC table. This table displays the interface name, VPI/VCI values, Mux type, and maximum protocols per AAL5.


Interface VPI VCI Mux Type Max Proto per AAL5 Conf. IL3 Protocol Actual IL3 Protocol Action(s)
aal5-1 0 63 - 0 Any None Reset IL3
aal5-0 8 35 LLC 2 Bridging and PPPoE PPPoE Reset IL3
Add Refresh Help

Click on the **trash can** icon to delete the current interface, or edit the current interface by clicking on the **pencil** icon.

Click on the **Add** button to another interface.

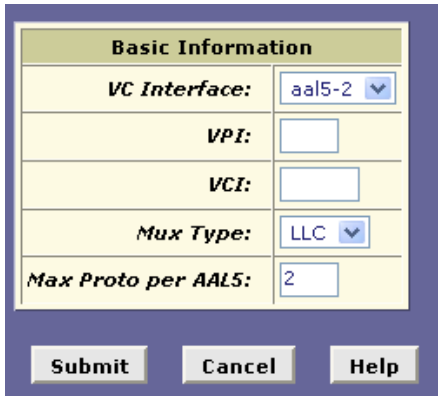
The devices WAN-side interfaces are used to communication via the DSL port. A WAN interface comprises two layers: a lower-level ATM VC interface and a higher-level protocol interface:

The ATM VC interface enables the device to communicate using the Asynchronous Transfer Mode protocol. The ATM protocol provides a common format for transmitting data over a variety of hardware systems that make up the backbone of the Internet. The virtual circuit (VC) properties of the ATM VC interface identify a unique path that your ADSL/Ethernet router uses to communicate via the ATM-based network with the telephone company central office equipment.

The higher-level protocol interface(s) operate "on top" of the ATM VC interface. The higher-level interface handles the protocols needed to log onto and exchange data with the ISP's access server. ISPs can use several different protocols, including the Point-to-Point Protocol (PPP), Ethernet-over-ATM (EoA) protocol, or the Internet Protocol-over-ATM (IPoA). Be sure to create the specific type of WAN interface your ISP requires.

After you have defined the ATM VC properties as described in this topic, you can configure one of the higher level WAN interfaces to enable communication with your ISP.

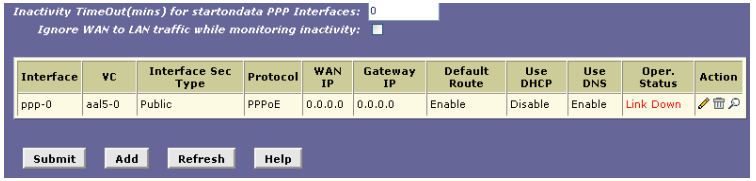
After you click on the **Add** button, another window will appear.



- **VC Interface**: The name of the lower-level interface on which this VC operates. The low-level interface names are preconfigured in the software and identify the type of traffic that can be supported, such as data or voice. Internet data services typically use an AAL5-type interface.
- **VPI, VCI, and Mux Type**: These settings identify a unique ATM data path for communication between your ADSL/Ethernet router and your ISP.
- **Max Proto per AAL5**: If you are using an AAL5-type of interface, this setting indicates the number of higher level interfaces that the VC can support (the higher level interfaces can be PPP, EoA, or IPoA interfaces). Contact your ISP to determine which connection protocol(s) they require.
- Click on the **Submit** button when completed and make sure to **Commit & Reboot**.

6.3 Point to Point Protocol (PPP)

Click on the **PPP** link to view the PPP configuration table. This table displays PPP information such as: interface name, interface type, protocol, WAN IP, gateway IP, default route, DHCP, DNS, and operation status.



Click on the **trash can** icon to delete the current interface, or edit the current interface by clicking on the **pencil** icon.

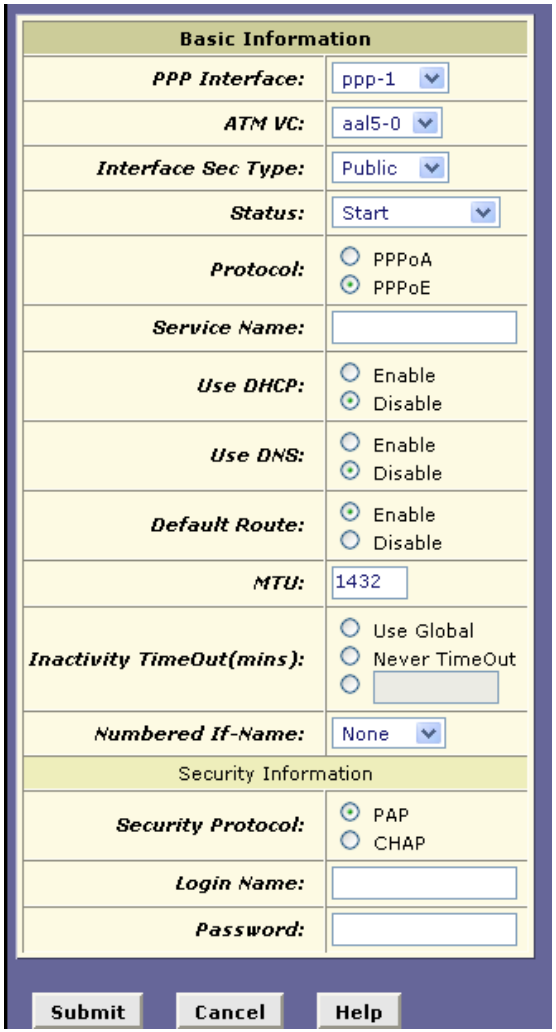
Click on the **Add** button to another interface.

The Point-to-Point Protocol (PPP) is one of several protocols used to enable communication between ISPs and their customers. PPP performs tasks such as the following:

- Identifying the type of service the ISP provides to a given customer
- Identifying the customer to the ISP through a username and password login
- Enabling the ISP to assign Internet information to the customer's computers

PPP can be used only when your connection with your ISP is a routed connection, not with a bridged connection.

After you click on the **Add** button, another window will appear.



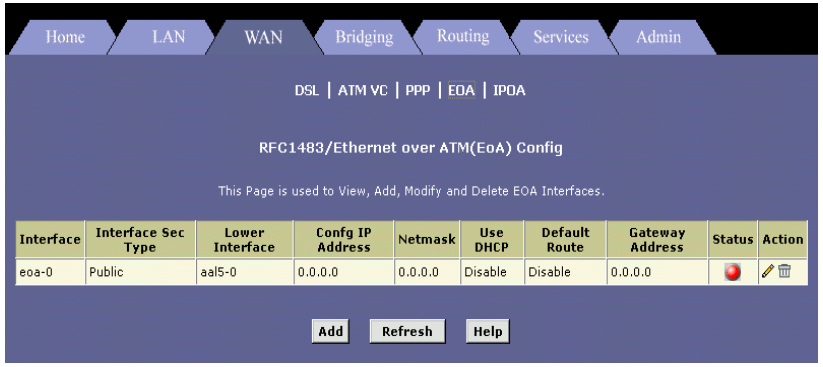
- **PPP Interface**: The predefined name of the PPP interface.
- **ATM VC**: The Virtual Circuit over which this PPP data is sent. The VC identifies the physical path the data takes to reach your ISP. See Configuring the ATM VC for more information.
- **Interface Sec Type**: The type of Firewall protections that are in effect on the interface (public, private, or DMZ): A public interface connects to the Internet (PPP interfaces are typically public). Packets received on a public interface are

subject to the most restrictive set of firewall protections defined in the software. A private interface connects to your LAN, such as the Ethernet interface. Packets received on a private interface are subject to a less restrictive set of protections, because they originate within the network. The term DMZ (de-militarized zone), in Internet networking terms, refers to computers that are available for both public and in-network accesses (such as a company's public Web server). Packets incoming on a DMZ interface -- whether from a LAN or external source -- are subject to a set of protections that is in between public and private interfaces in terms of restrictiveness.

- **Protocol**: The type of PPP protocol used. Your ISP may use PPP-over-Ethernet (PPPoE) or PPP-over-ATM (PPPoA).
- **Default Route**: Indicates whether the ADSL/Ethernet router should use the IP address assigned to this connection as its default route. Can be Enabled or Disabled. See Configuring IP Routes for an explanation of default routes.
- **MTU:** The Maximum Transmission Unit specifies the size in bytes of the largest Ethernet packet that the interface will accept. Packets larger than this size will be dropped.
- **Use DHCP**: When set to Enable, the device will acquire additional IP information from the ISP's DHCP server. The PPP connection itself acquires the device's IP address, mask, DNS address, and default gateway address. With Use DHCP enabled, the device will acquire IP addresses for various other server types (WINS, SMTP, POP3, etc. -- these server types are listed on the DHCP Server Configuration page).
- **Use DNS**: When set to Enable, the DNS address learned through the PPP connection will be distributed to clients of the device's DHCP server. This option is useful only when the ADSL/Ethernet Router is configured to act as a DHCP server for your LAN.
- **Security Protocol**: Select a security protocol and then enter the user name and password.
- Click on the **Submit** button when completed and make sure to **Commit & Reboot**.

6.4 Ethernet over ATM (EoA)

Click on the **EOA** link to view the RFC1483/EoA configuration table. This table displays EoA information such as: interface name, interface security type, lower interface, config IP, network IP, DHCP, default route, gateway IP, and status.



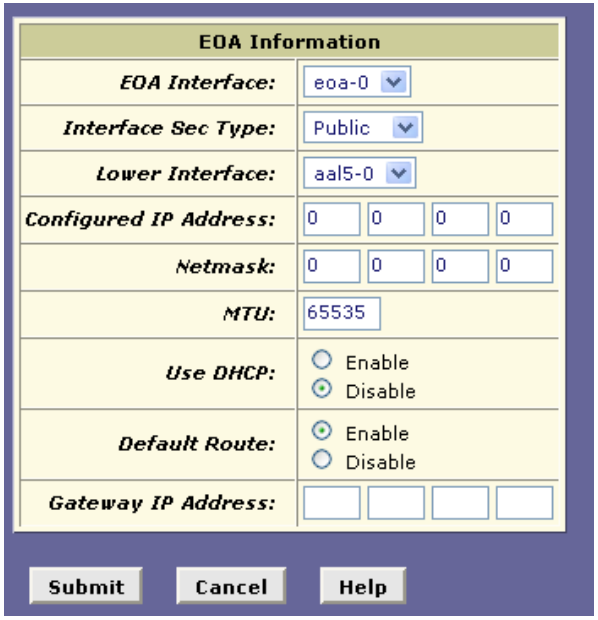
Click on the **trash can** icon to delete the current interface, or edit the current interface by clicking on the **pencil** icon.

Click on the **Add** button to add another interface.

The Ethernet-over-ATM (EoA) protocol is commonly used to carry data between local area networks that use the Ethernet protocol and wide-area networks that use the ATM protocol. Many telecommunications industry networks use the ATM protocol. ISPs who provide DSL services often use the EoA protocol for data transfer with their customers' DSL modems.

EoA can be implemented to provide a bridged connection between a DSL modem and the ISP. In a bridged connection, data is shared between the ISP's network and their customer's as if the networks were on the same physical LAN. Bridged connections do not use the IP protocol. EoA can also be configured to provide a routed connection with the ISP, which uses the IP protocol to exchange data.

After you click on the **Add** button, another window will appear.

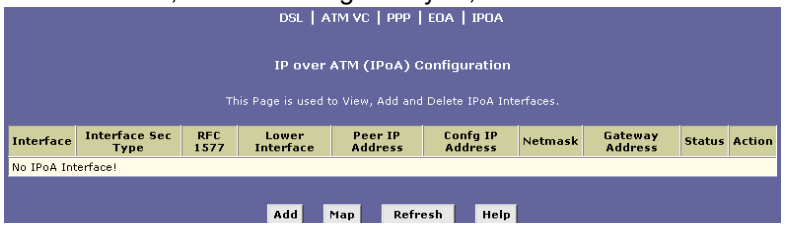


- **EOA Interface**: The name the software uses to identify the EoA interface.
- **Interface Sec Type**: The type of security protections in effect on the interface (public, private, or DMZ): A public interface connects to the Internet (IPoA interfaces are typically public). Packets received on a public interface are subject to the most restrictive set of firewall protections defined in the software.A private interface connects to your LAN, such as the Ethernet interface. Packets received on a private interface are subject to a less restrictive set of protections, because they originate within the network. The term DMZ (de-militarized zone), in Internet networking terms, refers to computers that are available for both public and in-network accesses (such as a company's public Web server). Packets incoming on a DMZ interface -- whether from a LAN or external source -- are subject to a level of protection that is in between those for public and private interfaces.

- **Lower interface**: EoA interfaces are defined in software, and then associated with lower-level software and hardware structures (at the lowest level, they are associated with a physical port - the WAN port). This field should reflect an interface name defined in the next lower level of software over which the EoA interface will operate. This will be an ATM VC interface, such as aal5-0, as described in Configuring the ATM VC.
- **Config IP Address and Net Mask**: The IP address and network mask you want to assign to the interface. If the interface will be used for bridging with your ISP and you will not be using the device as a router on your LAN, then you do not need to specify IP information. If you enable DHCP for this interface, then the Configured IP address will serve only as a request to the DHCP server. The actual address that is assigned by the ISP may differ if this address is not available.
- **Use DHCP**: When enabled, this setting instructs the device to accept IP information assigned dynamically by your ISP's DHCP server. If the interface will be used for bridging with your ISP and you will not be routing data through it, leave this checkbox unselected.
- **Default Route**: Indicates whether the ADSL/Ethernet router should use the IP address assigned to this interface, if any, as its default route for your LAN. This can be Enable or Disable. See Configuring IP Routes for an explanation of default routes.
- **Gateway Address**: The external IP address that the ADSL/Ethernet router communicates with via the EoA interface to gain access to the Internet. This is typically an ISP server.
- Click on the **Submit** button when completed and make sure to **Commit & Reboot**.

6.5 IP over ATM (IPoA)

Click on the **IPoA** link to view the IP over ATM configuration table. This table displays IPoA information such as: interface name, interface security type, lower interface, config IP, network IP, subnet mask gateway IP, and status.

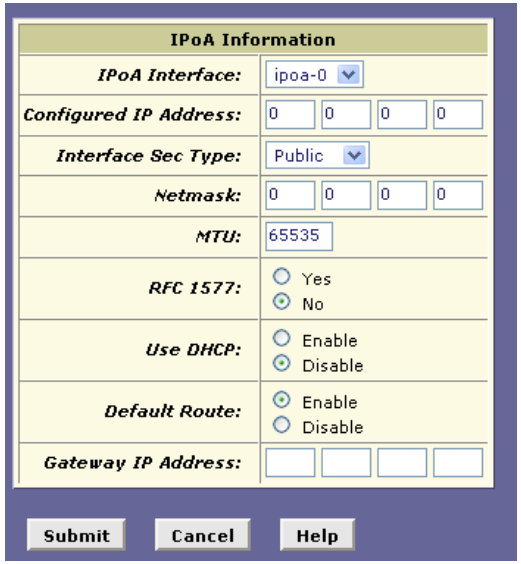


Click on the **trash can** icon to delete the current interface, or edit the current interface by clicking on the **pencil** icon.

Click on the **Add** button to add another interface.

An IPoA interface can be used to exchange IP packets over the ATM network, without using an underlying Ethernet over ATM (EOA) connection. Typically, this type of interface is used only in product development environments, to eliminate unneeded variables when testing IP layer processing.

After you click on the **Add** button, another window will appear.



- **IPoA Interface**: The name the software uses to identify the IPoA interface
- **Config IP Address and Net Mask**: The IP address and network mask you want to assign to the interface. If the interface will be used for bridging with your ISP and you will not be using the device as a router on your LAN, then you do not need to specify IP information. If you enable DHCP for this interface, then the Configured IP address will serve only as a request to the DHCP server. The actual address that is assigned by the ISP may differ if this address is not available.
- **Interface Security Type**: The type of firewall protections that are in effect on the interface (public, private, or DMZ): A public interface connects to the Internet (IPoA interfaces are typically public). Packets received on a public interface are subject to the most restrictive set of firewall protections defined in the software. A private interface connects to your LAN, such as the Ethernet interface. Packets received on a private interface are subject to a less restrictive set of protections, because they originate within the network. The term DMZ (de-militarized zone), in Internet networking terms, refers to computers that are available for both public

and in-network accesses (such as a company's public Web server). Packets incoming on a DMZ interface -- whether from a LAN or external source -- are subject to a level of protection that is in between public and private interfaces in terms of restrictiveness.

- **RFC 1577**: Specifies whether the IPoA protocol to be used complies with the IEFT specification named "RFC 1577 - Classical IP and ARP over ATM" (contact your ISP if unsure).
- **Lower interface**: An IPoA interface must be associated with one or more ATM VCs that have been defined on the system. The ATM VC is also considered an interface--one that performs "lower level" functions (i.e., closer to hardware) than the IPoA interface. See Configuring the ATM VC for information about ATM VC interfaces.
- **Gateway Address**: The external IP address that the ADSL/Ethernet router communicates with via the IPoA interface to gain access to the Internet. This is typically an ISP server.
- Click on the **Submit** button when completed and make sure to **Commit & Reboot**.

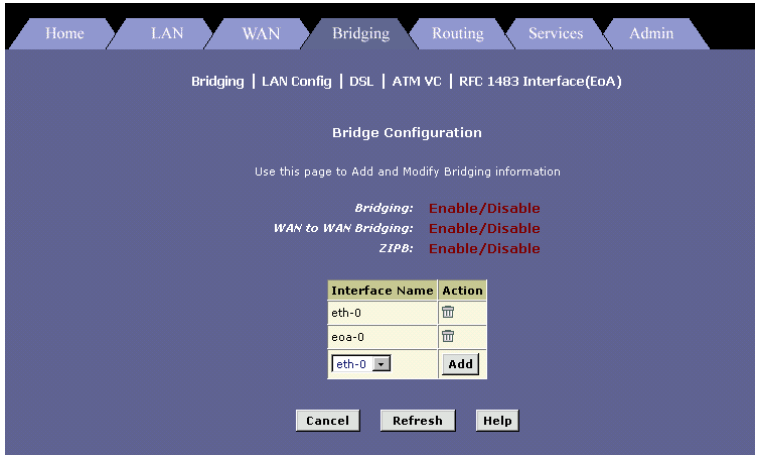
7 Bridging

Click on the **Bridging** tab to view its sub-menu's and configure the bridge settings. The six sub-menu's are: Bridging, LAN Config, DSL, ATM VC, and RFC 1483 Interface (EoA). The bridging sub-menu is described below. (*Each of the other sub-menus is described in the earlier sections.)*

7.1 Bridging

Click on the **Bridging** link to view the Bridge configuration. This table displays bridge information such as: interface name.

Click on the **trash can** icon to delete the current interface, or edit the current interface by clicking on the **pencil** icon.
There are three radio buttons on this page. In order to use bridging, you must enable **Bridging** and **WAN to WAN Bridging**.



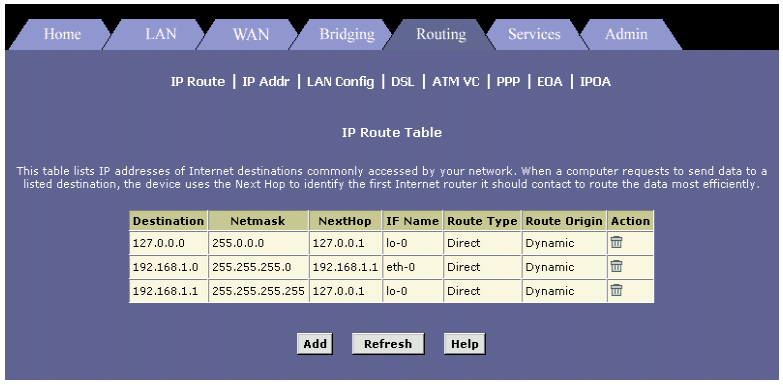
8 Routing

Click on the **Routing** tab to view its sub-menu's and configure the routing settings. The eight sub-menu's are: IP route, IP address, LAN Config, DSL, ATM VC, PPP, EoA, and IPoA. The IP route sub-menu is described below. (*Each of the other sub-menus is described in the earlier sections.)*

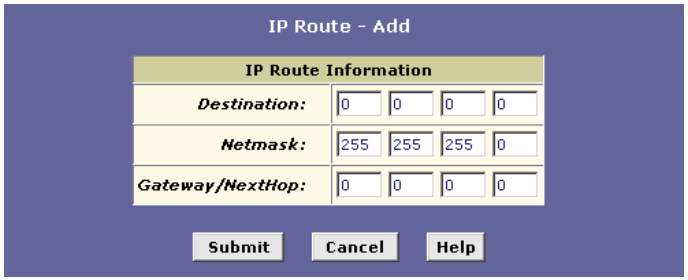
8.1 IP Route

Click on the **IP Route** link to view the IP route table. This table displays IP route information such as: destination, net mask, next hop, interface name, route type and route origin. This table lists IP addresses of Internet destinations commonly accessed by your network. When a computer requests to send data to a listed destination, the device uses the Next Hop to identify the first Internet router it should contact to route the data most efficiently.

Click on the **trash can** icon to delete the current destination or click on the **Add** button to add another destination.


Home
LAN
WAN
Bridging
Routing
Services
Admin
IP Route | IP Addr | LAN Config | DSL | ATM VC | PPP | EOA | IPOA
IP Route Table
This table lists IP addresses of Internet destinations commonly accessed by your network. When a computer requests to send data to a listed destination, the device uses the Next Hop to identify the first Internet router it should contact to route the data most efficiently.
Destination
Netmask
NextHop
IF Name
Route Type
Route Origin
Action
127.0.0.0 255.0.0.0 127.0.0.1 lo-0 Direct Dynamic
192.168.1.0 255.255.255.0 192.168.1.1 eth-0 Direct Dynamic
192.168.1.1 255.255.255.255 127.0.0.1 lo-0 Direct Dynamic
Add
Refresh
Help

After you click on the **Add** button, another window will pop-up.



- **Destination**: Specifies the IP address of the destination computer. The destination can specified as the IP address of a specific computer or an entire network. It can also be specified as all zeros to indicate that this route should be used for all destinations for which no other route is defined (this is the route that creates the default gateway).
- **Netmask**: Indicates which parts of the destination address refer to the network and which parts refer to a computer on the network. The default gateway uses a netmask of 0.0.0.0.
- **NextHop**: Specifies the next IP address to send data to when its final destination is that shown in the destination column.
- Click on the **Submit** button when completed and make sure to **Commit & Reboot**.

9 Services

Click on the **Services** tab to view its sub-menu's and configure the service settings. The six sub-menu's are: NAT, RIP, Firewall, IP filter, DNS, and Blocked Protocols, DDNS, and UPNP. Each one is described in detail below.

9.1 NAT

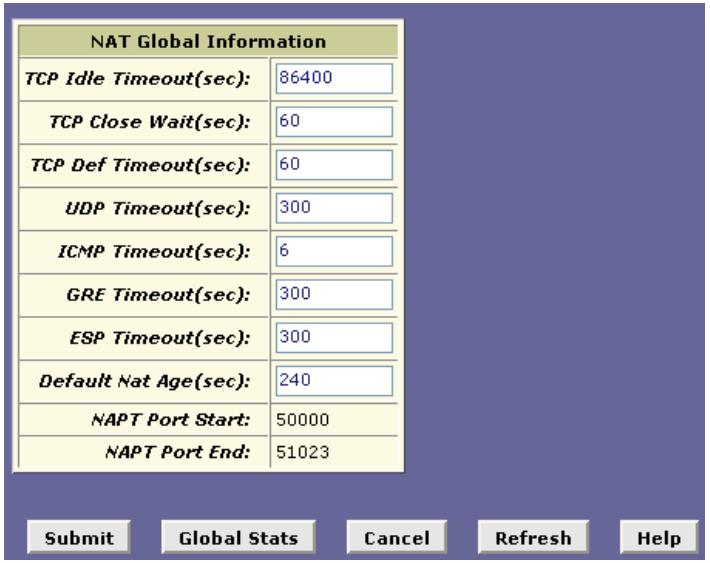
Click on the **NAT** link to view the NAT global information table. Network Address Translation is a method for disguising the private IP addresses you use on your LAN as the public IP address you use on the Internet. You define NAT rules that specify exactly how and when to translate between public and private IP addresses.

The NAT feature offers three sections. First, click on the **Enable** radio box, to enable the NAT feature. Then select a NAT option from the drop down list.

The three options are: NAT Global Info, NAT Rule Entry, and NAT translations. Each one is described below.

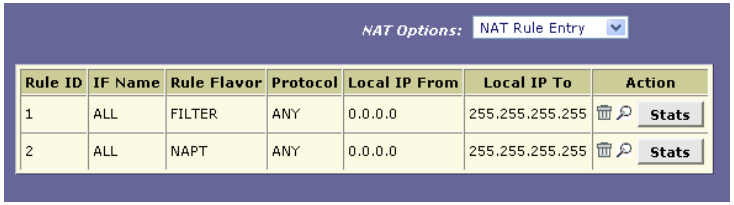
a) NAT Global Info

The table displays the idle times for several protocols; you may change the times and then click on the **Submit** button.

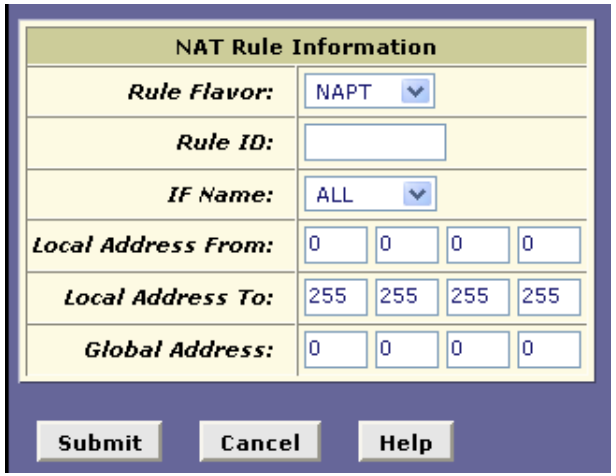


b) NAT Rule Entry

The table displays NAT route configuration. Click on the **trash can** icon to delete the current rule or click on the **Add** button to add another rule.



After you click on the **Add** button, another window will appear.

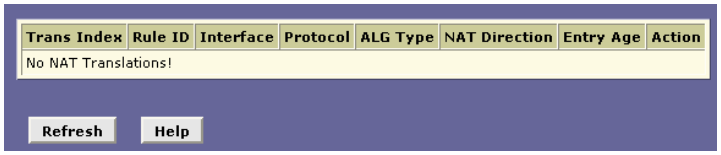


- **Rule Flavor**: Select NAPT from the drop-down list.
- **Rule ID**: The Rule ID determines the order in which rules are invoked (the lowest numbered rule is invoked first, and so on). In some cases, two or more rules may be defined to act on the same set of IP addresses. Be sure to assign the Rule ID so that the higher priority rules are invoked before lower-priority rules. It is recommended that you select rule IDs as multiples of 5 or 10 so that, in the future, you can insert a rule between two existing rules. When a data packet matches a rule, the data is acted upon according to that rule and is not subjected to higher-numbered rules.
- **IF Name**: Select an interface name from the drop-down list.

- **Local Address From/To**: Enter the the starting and ending IP addresses of the range of private address you want to be translated. You can specify that data from all LAN addresses should be translated by typing 0 (zero) in each From field and 255 in each To field. Or, type the same address in both fields if the rule only applies to one LAN computer.
- **Global Address**: Enter the public IP address which was assigned by the ISP.
- Click on the **Submit** button when completed and make sure to **Commit & Reboot**.

c) NAT Translations

The table displays the current NAT translations, if any exist. Click on the **trash can** icon to delete a translation or click on the **Refresh** button to refresh the page.



- **Trans Index**: The sequential number assigned to the IP session used by this NAT translation session.
- **Rule ID**: The ID number of the NAT rule.
- **Interface**: The interface name on which the NAT rule was invoked.
- **Protocol**: Lists the protocols used by data packets that are currently under translation.
- **ALG Type**: The Application Level Gateway (ALG), if any, that was used to enable this NAT translation (ALGs are special settings that certain applications require in order to work while NAT is enabled).
- **NAT Direction**: The direction (incoming or outgoing) of the translation. A NAT direction is assigned to each port; the Ethernet and USB interfaces are defined as inside interfaces, and the WAN interfaces are defined as outside interfaces. The NAT direction is determined by the interface on which the rule is invoked.
- **Entry Age**: The elapsed time, in seconds, of the NAT translation session.

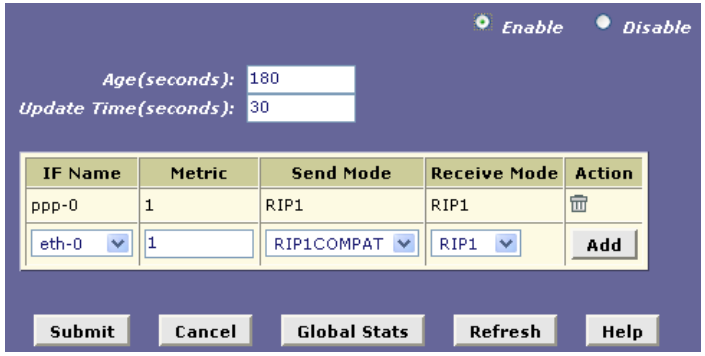
9.2 RIP

Click on the **RIP** link to view the Routing Information Protocol (RIP) Configuration table. Routers on your LAN communicate with one another using the Routing Information Protocol.

RIP is an Internet protocol you can set up to share routing table information with other routing devices on your LAN, at your ISP's location, or on remote networks connected via the ADSL line. Generally, RIP is used to enable communication on autonomous networks. An autonomous network is one in which all the computers are administered by the same entity. An autonomous network may be a single network, or a grouping of several networks under the same administration. An example of an autonomous network is a corporate LAN, including devices that can access it from remote locations, such as the computers telecommuters use.

Using RIP, each device sends its routing table to its closest neighbour every 30 seconds. The neighbouring device in turn passes the information on to its next neighbour and so on until all devices in the autonomous network have the same set of routes.

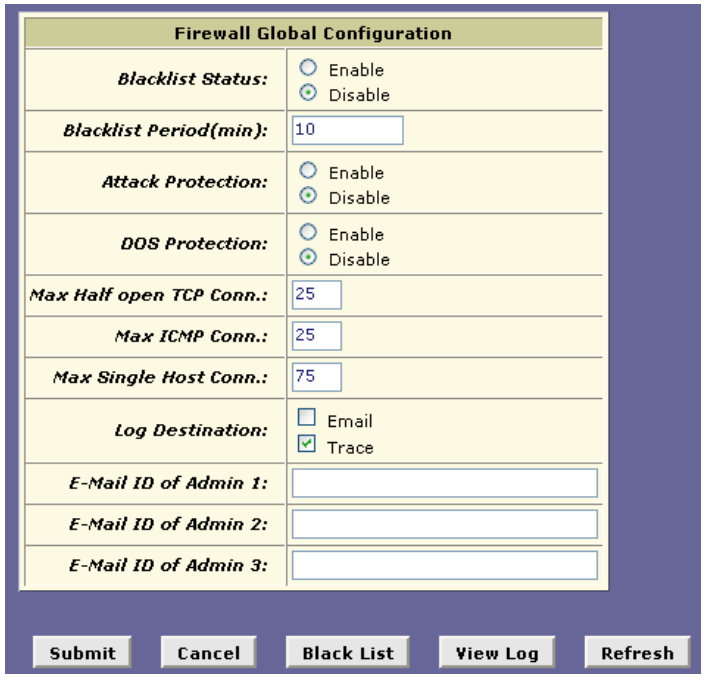
This table lists any interfaces on your device that use RIP (typically the LAN interface), and the version of the protocol used. Click on the **trashcan** icon to delete a RIP interface. Click on the **Global Stats** icon to view the NAT statistics. This table will open in a new window.



- **RIP Status**: Select the **Enable** or **Disable** radio button in order to use the protocol.
- **Age**: This s the amount of time in seconds that the device's RIP table will retain each route that it learns from adjacent computers.
- **Update Time**: This specifies how frequently the ADSL/Ethernet router will send out its routing table to its neighbours.
- **IF Name**: Select an interface name from the drop-down list.
- **Metric**: Enter a metric value. RIP uses a hop count as a way to determine the best path to a given destination in the network. The hop count is the sum of the metric values assigned to each port through which data is passed before reaching the destination. Among several alternative routes, the one with the lowest hop count is considered the fastest path. For example, if you assign this port a metric of 1, then RIP will add 1 to the hop count when calculating a route that passes through this port. If you know that communication via this interface is slower than through other interfaces on your network, you can assign it a higher metric value than the others. You can select any integer from 1 to 15.
- **Send/Receive Mode:** Select a Send and Receive mode from the drop-down list. The Send Mode setting indicates the RIP version this interface will use when it sends its route information to other devices. The Receive Mode setting indicates the RIP version(s) in which information must be passed to the ADSL/Ethernet router in order for it to be accepted into its routing table. RIP version 1 is the original RIP protocol. Select RIP1 if you have devices that communicate with this interface that understand RIP version 1 only. RIP version 2 is the preferred selection because it supports "classless" IP addresses (which are used to create subnets) and other features. Select RIP2 if all other routing devices on your LAN support this version of the protocol.
- Click on the **Submit** button when completed and make sure to **Commit & Reboot**.

9.3 Firewall

Click on the **Firewall** link to view the Firewall Configuration table. The Firewall adds security to your network by protecting it from Internet intruders.



- **Blacklist Status**: Select **Enable** if you would like the device to maintain a blacklist.
- **Blacklist Period (min)**: Specifies the number of minutes that a computer's IP address will remain on the black list (i.e., all traffic originating from that computer will be blocked from passing through any interface on the ADSL/Ethernet router).
- **Attack Protection**: Select the Enable radio button to use the built-in firewall protections that prevent the following common types of attacks: **IP Spoofing** - sending packets over the WAN interface using an internal LAN IP address as the source address. **Tear Drop** - sending packets that contain overlapping fragments. **Smurf and Fraggle** -

sending packets that use the WAN or LAN IP broadcast address as the source address. **Land Attack** - sending packets that use the same address as the source and destination address. **Ping of Death** - illegal IP packet length.

- **DOS Protection**: Click on the Enable button to use the following Denail of Service protection: SYN DoS, ICMP DoS, Per-host DoS protection.
- **Max Half open TCP Connection**: Enter the percentage of concurrent IP sessions that can be in the half-open state. In ordinary TCP communication, packets are in the half-open state only briefly as a connection is being initiated; the state changes to active when packets are being exchanged, or closed when the exchange is complete. TCP connections in the half-open state can use up the available IP sessions. If the percentage is exceeded, then the half-open sessions will be closed and replaced with new sessions as they are initiated.
- **MAX ICMP Connection**: Sets the percentage of concurrent IP sessions that can be used for ICMP messages. If the percentage is exceeded, then older ICMP IP sessions will be replaced by new sessions as the are initiated.
- **Max Single Host Connection**: Sets the percentage of concurrent IP session that can originate from a single computer. This percentage should take into account the number of hosts on the LAN.
- **Log Destination**: Select how attempted violations of the firewall settings will be tracked. Records of such events can be sent via Ethernet to be handled by a system utility (Trace) or can e-mailed to specified administrators.
- **Email ID of Admin**: Enter the e-mail addresses of the administrators who should receive notices of any attempted firewall violations.
- Click on the **Submit** button when completed and make sure to **Commit & Reboot**.

.

9.4 IP Filter

Click on the IP Filter link to view the IP filter configuration table. The IP filter feature enables you to create rules that control the forwarding of incoming and outgoing data between your LAN and the Internet and within your LAN.

You can create IP filter rules to block attempts by certain computers on your LAN to access certain types of data or Internet locations. You can also block incoming access to computers on your LAN.

When you define an IP filter rule and enable the feature, you instruct the ADSL/Ethernet router to examine data packets to determine whether they meet criteria set forth in the rule. The criteria can include the network or internet protocol the packet carries, the direction in which it is traveling (for example, from the LAN to the Internet or vice versa), the IP address of the sending computer, the destination IP address, and other characteristics of the packet data.

If the packet matches the criteria established in a rule, the packet can either be accepted (forwarded towards its destination), or denied (discarded), depending on the action specified in the rule.

IP Filter Configuration
This Page is used to View and Modify IP Filter Global and Rule Configuration.
Security Level: None
Public Default Action: Accept
Private Default Action: Deny
DMZ Default Action: Accept

- **Security Level**: Select **None, Medium, Low,** or **High.** This setting determines which IP Filter rules take effect, based on the security level specified in each rule. For example, when **High** is selected, only those rules that are assigned a security value of High will be in effect. The same is true for the **Medium** and **Low** settings. When **None** is selected, IP Filtering is disabled.
- **Private/Public/DMZ Default Action**: This setting specifies a default action to be taken (Accept or Deny) on private, public, or DMZ-type device interfaces when they receive packets that do not match any of the filtering rules. You can specify a different default action for each interface type. A

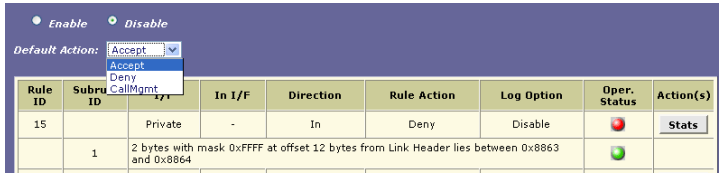
public interface typically connects to the Internet. PPP, EoA, and IPoA interfaces are typically public. Packets received on a public interface are subject to the most restrictive set of firewall protections defined in the software. Typically, the global setting for public interfaces is Deny, so that all accesses to your LAN initiated from external computers are denied. A **private** interface connects to your LAN, such as the Ethernet interface. Packets received on a private interface are subject to a less restrictive set of protections, because they originate within the network. Typically, the global setting for private interfaces is Accept, so that LAN computers have access to the ADSL/Ethernet routers' Internet connection. The term **DMZ** (de-militarized zone), in Internet networking terms, refers to computers that are available for both public and in-network accesses (such as a company's public Web server). Packets received on a DMZ interface -- whether from a LAN or external source -- are subject to a set of protections that is in between public and private interfaces in terms of restrictiveness. The global setting for DMZ-type interfaces may be set to Deny so that all attempts to access these servers are denied by default; the administrator may then configure IP Filter rules to allow accesses of certain types.

9.5 Bridge Filter

Click on the **Bridge Filter** link to view the bridge filter configuration table. Bridge filter rules can be created to control the forwarding of incoming and outgoing data between your LAN and the Internet and within your LAN. Bridge filter rules make decisions based on the structure of the "layer 2" data packets (e.g., Ethernet packets) received on the device interfaces, unlike IP filter rules, which are based on the structure of "layer 3" (e.g., IP) packets.

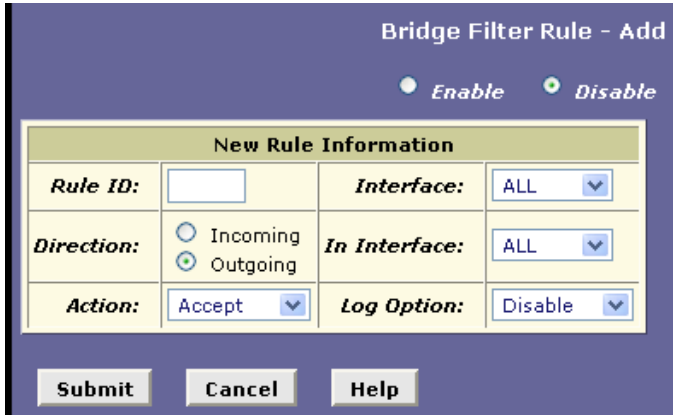
When the bridge filtering feature is enabled, the bridge/router examines each incoming layer 2 packet and compares it to the bridge filter rules. The bridge filter rules specify which bits of the packet are to be examined, and what criteria those bits must meet in order to qualify as a match for the rule.

When a packet matches a rule, it can either be accepted (forwarded towards its destination), or denied (discarded), depending on the action specified in the rule.



- **Bridge Filter**: Click on the **Enable** or **Disable** radio button to activate/deactivate the service. Although each rule is independently enabled and disabled, no rules will be effective unless the Enable radio button is selected here.
- **Default Action:** Select **Accept** or **Deny** from the drop-donw list. By accepting or denying this action will affect all packets on all interfaces.
- Click on the **Submit** button when completed and make sure to **Commit & Reboot**.

Click on the **Add** button to add a bridge filter rule.



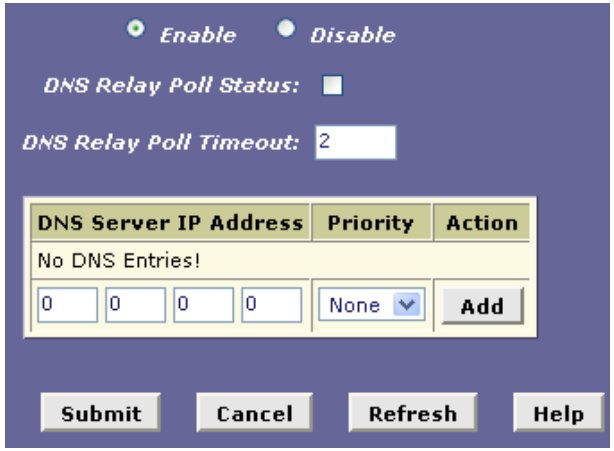
- **Rule ID:** Each rule must be assigned an ID number. Rules are processed from lowest to highest on each data packet, until a match is found. Rule numbers up to 99 are reserved for preconfigured system rules. **Rule IDs must start at 1000 or above so that they do not interfere with system-defined rules.** It is also recommended that you assign rule IDs in multiples of 5 or 10 (e.g., 1000, 1010, 1020) so that you leave enough room between them for inserting new rules if necessary.
- **Interface**: Enter the interface name on which the rule will take effect.
- **Direction**: Specifies whether the rule should apply to packets that are incoming or outgoing on the selected interface. **Incoming** refers to packets coming in to the LAN on the interface, and **Outgoing** refers to packets going out from the LAN. You can use rules that specify the incoming direction to restrict external computers from accessing your LAN.
- **In Interface**: The interface from which packets must be forwarded in order for this rule to be invoked. For example, if the Interface criteria is set to *ppp-0*, then the In Interface could be set to *usb-0*. This specifies that the rule applies only to packets passed from the USB computer through the router's PPP interface. This option is valid only for rules defined for the outgoing direction.
- **Action**: Specifies what the rule will do to a packet when the packet matches the rule criteria. The action can be **Accept** (forward to destination) or **Deny** (discard the packet). Do not select the CallMgt option.
- **Log Option**: When **Enabled** is selected, a log entry will be created on the system each time this rule is invoked. Logging may be helpful when troubleshooting. You can also **disable** logging, log only packets that match rules, or log only packets that do not match rules.
- Click on the **Submit** button when completed and make sure to **Commit & Reboot**.

9.6 Domain Name Service (DNS)

Click on the **DNS** link to view the DNS Configuration table. This page is used for adding and deleting DNS server IP addresses.

Domain Name System (DNS) servers map the user-friendly domain names that users type into their Web browsers (e.g., "yahoo.com") to the equivalent numerical IP addresses that are used for Internet routing.

When a PC user types a domain name into a browser, the PC must first send a request to a DNS server to obtain the equivalent IP address. The DNS server will attempt to look up the domain name in its own database, and will communicate with higher-level DNS servers when the name cannot be found locally. When the address is found, it is sent back to the requesting PC and is referenced in IP packets for the remainder of the communication.

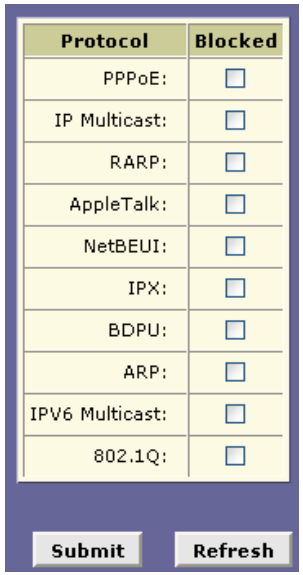


- Click on the **Enable** or **Disable** radio button to manage the DNS feature.
- **DNS Relay Poll Status:** By placing a check in this box the software will send out regular test messages to the DNS servers to make sure that they remain up.
- **DNS Relay Poll Timeout:** Enter a value (number of minutes) after which the polling of the DNS server will time out.
- **DNS Server IP Address:** Enter the DNS server IP address.
- **Priority:** Select a priority level from the drop-down list.
- Click on the **Add** button to add the entry into the table.
- Click on the **Submit** button when completed and make sure to **Commit & Reboot**.

9.7 Blocked Protocols

Click on the **Blocked Protocols** link to view the list of protocols. This page is used to block or unblock protocols running across the system. Place a check in the box of particular protocol in order to block it.

The ADSL/Ethernet router is capable of sending and receiving information in a variety of protocol formats. The Blocked Protocols feature enables you to prevent the ADSL/Ethernet router from passing any data that uses a particular protocol. Unlike the IP Filter feature, you cannot specify additional criteria for blocked protocols, such as particular users or destinations. However, when you are certain that a particular protocol is not needed or wanted on your network, this feature provides a convenient way to discard such data before it is passed.



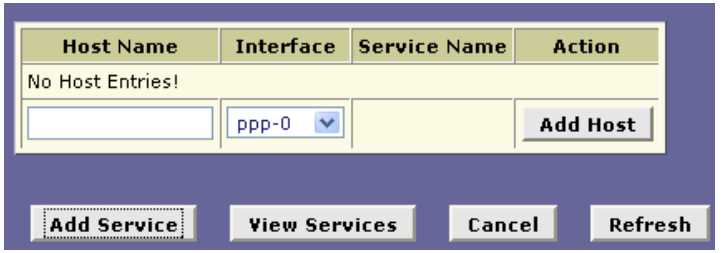
Note: Blocking certain protocols may disrupt or disable your network communication or Internet access. If you are unfamiliar with how your network or Internet connection uses these protocols, contact your ISP before disabling.

- **PPPoE:** Point to Point Protocol over Ethernet. Many DSL modems use PPoE to establish and maintain a connection with a service provider. PPoE provides a means of logging in to the ISPs servers so that they can authenticate you as a customer and provide you access to the Internet. Check with your ISP before blocking this protocol.
- **IP Multicast**: IP Multicast is an extension to the IP protocol. It enables individual packets to be sent to multiple hosts on the Internet, and is often used for handling e-mail mailing lists and teleconferencing and videoconferencing.

- **RARP**: Reverse Address Resolution Protocol. This IP protocol provides a way for computers to determine their own IP addresses when they only know their hardware address (i.e., MAC addresses). Certain types of computers, such as diskless workstations, must use RARP to determine their IP address before communicating with other network devices.
- **AppleTalk**: A networking protocol used in for Apple Macintosh® networks.
- **NetBEUI**: NetBIOS Enhanced User Interface. On many LAN operating systems, the NetBEUI protocol provides the method by which computers identify themselves to and communicate with each other.
- **IPX**: Internetwork Packet Exchange. A networking protocol used on Novell Netware ®-based LANs.
- **BDPU**: Bridge Protocol Data Unit. BPDUs are data messages that are exchanged across the switches between LANs that are connected by a bridge. BPDU packets contain information on ports, addresses, priorities and costs, and are exchanged across bridges to detect and eliminate loops in a network.
- **ARP**: Address Resolution Protocol. Computers on a LAN use ARP to learn the hardware addresses (i.e., MAC addresses) of other computers when they know only their IP addresses.
- **IPV6 Multicast**: IP Multicasting under IP Protocol version 6. IP Multicast is an extension to the IP protocol. It enables individual packets to be sent to multiple hosts on the Internet, and is often used for handling e-mail mailing lists and teleconferencing and videoconferencing.
- **802.1Q:** This IEEE specification defines a protocol for virtual LANs on Ethernet networks. A virtual LAN is a group of PCs that function as a local area network, even though the PCs may not be physically connected. They are commonly used to facilitate administration of large networks.
- Click on the **Submit** button when completed and make sure to **Commit & Reboot**.

9.8 DDNS

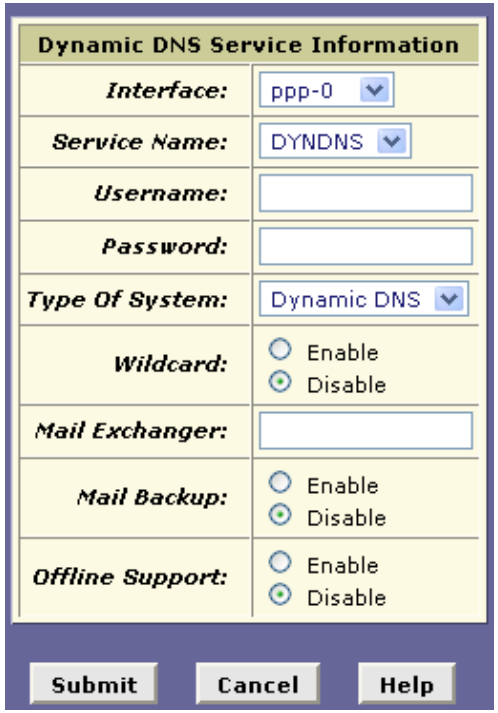
Click on the **DDNS** link to configure and add dynamic DNS entries. Dynamic DNS (DDNS) is a service that facilitates outside Internet access to a LAN host even when the host's dynamically-assigned IP address changes frequently.



DDNS is useful when you have a host (running for example, a web server) that receives a dynamically assigned IP address from a DHCP server. A user on the Internet would typically access the host by entering its name in their web browser. A DNS server on the web would then resolve the name to its associated numeric IP address, as required for Internet protocol processing. However, when a host's IP address is dynamically assigned (for example, by a DHCP server), it may change frequently. In this scenario, a DNS server may have outdated data and may not be able to resolve a host name to the current IP address.

When a host is registered with a DDNS service provider, the provider is automatically notified by the host of any change in its IP address and the provider then propagates the change throughout the DNS server system.

Click on the **Add Service** button to a new DDNS entry.



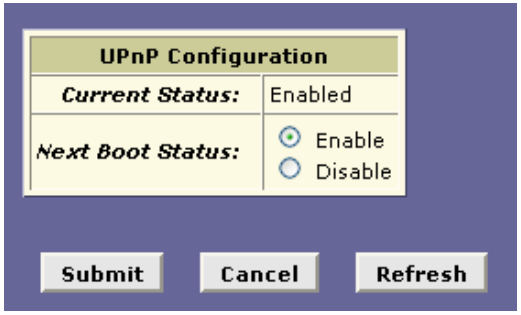
- **Interface:** Select an interface from the drop-down list. Specifies the public device interface. You can specify only one DDNS service on each interface.
- **Service Name:** Select the DDNS service provider from the drop-down list for which the host names of the interface have been registered. **DYDNS** (Dynamic Network Servicves, Inc.) or **TZO** (Tzolkin Corporation).
- **Username/Password:** Enter the username and password for the DDNS service.
- **Type of System**: Select a type of system from the drop-down list: **Dynamic DNS**, **Static DNS**, or **Custom DNS**. **Dynamic DNS** associates your hostname with the ISP-assigned dynamic IP address, updates the IP address when notified of changes, and propagates the update throughout the DNS server system. **Static DNS** associates your hostname with your ISP-assigned static IP address. Although automatic updates are allowed, changes to the IP address are expected to be less frequent, and will take longer to propagate though the DNS system. **Custom DNS**

is a full DNS solution for newly purchased domains or domains you already own. A web-based interface provides complete control over resource records and your entire domain, including support for dynamic IP addresses and automated updates. You can create different domains in these systems.

- **Wildcard:** Specifies whether the service provider can use a wildcard DNS record to resolve variations on the host name to the associated IP address. When enabled, a wildcard record of DNS record type CNAME is used to resolve queries for addresses of the form *.yourhost.ourdomain.ext to the same IP address as found in the DNS record for yourhost.ourdomain.ext.
- **Mail Exchanger:** Specifies a Mail Exchanger (MX) server name to use for e-mails addressed to the hostname. The specified MX must resolve to an IP address or it will be ignored. Providing no MX setting (or an MX that does not resolve properly to a DNS record of type A) causes the hostname's MX record(s) to be removed.
- **Mail Backup:** Specifies whether or not e-mails are to be backed up by the service provider.
- **Offline Support:** Specifies whether or not users will be redirected to a designated service provider site when the host computer is not available.
- Click on the **Submit** button when completed and make sure to **Commit & Reboot**.

9.9 UPNP

Click on the **UPNP** link to enable the Universal Plug and Play settings. Click on the **Enable** button to enable UPNP and then click on the **Submit** button.



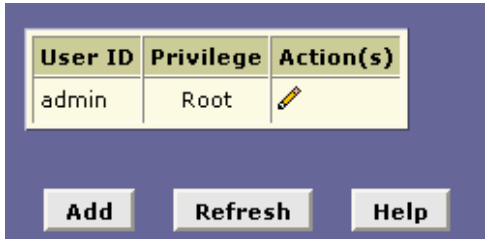
10 Admin

Click on the **Admin** tab to view its sub-menu's and configure the admin settings. The sub-menu's are: User Config, Commit & Reboot, Local Image Upgrade, Remote Image Upgrade, Alarm, Diagnostics, and Port Settings, System Log, Backup/Restore Config, Management Control, Autodetect, SNMP Config, and Parental Contraol . Each one is described in detail below.

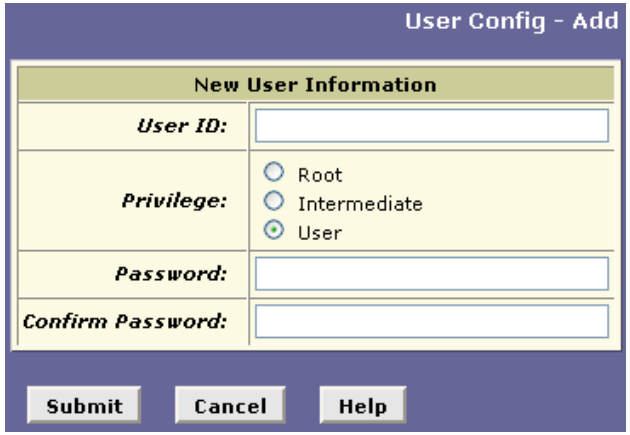
Home
LAN
WAN
Bridging
Routing
Services
Admin
User Config | Commit & Reboot | Local Image Upgrade | Remote Image Upgrade | Alarm | Diagnostics | Port Settings |
System Log | Backup/Restore Config | Management Control | Autodetect | SNMP Config | Parental Control

10.1 User Config

Click on the **User Config** link to view the list of users. This page displays user information. Use this page to add/delete users and change your password. Your new username and password can be up to 128 characters and is case-sensitive.



To add a new user click on the **Add** button, or click on the **pencil** icon to edit the settings of an existing user.



- **User ID:** Enter a new username.
- **Privilege**: Select a privilege level: **Root**, **Intermediate**, or **User**. **Root-level** privileges enable users to modify all the features available in Configuration Manager. The default login has root-level privileges. **Intermediate-level** privileges enable users to change their own passwords. They can also change the PPP interface username and password, and the ATM VC interface values. (Note, however, that Intermediate users can change these only on the PPP and ATM VC pages - not on the Quick Configuration page.) These users can view-but not create or modify- all other system information. **User-level** privileges enable users to change their own passwords. They can view -- but not create or modify -- all other system information.
- **Password/Confirm Password:** Enter and confirm a password. The password can be up to 128 characters in length and is case-sensitive.
- Click on the **Submit** button when completed and make sure to **Commit & Reboot**.

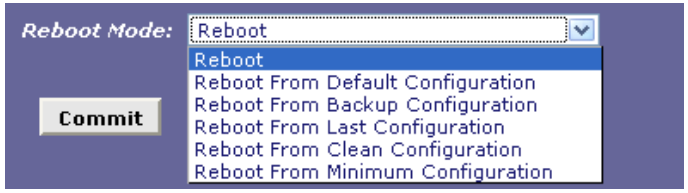
10.2 Commit & Reboot

Click on the **Commit & Reboot** link to view the reboot options. This page is used to save the changes into the device's memory and reboot the device using different options.

Click on the **Commit** button to save the changes.
In order to reboot the device, select and option from the drop down list. The six options are:

a. Reboot
b. Reboot from default configuration
c. Reboot from backup configuration
d. Reboot from last configuration
e. Reboot from clean configuration
f. Reboot from minimum configuration

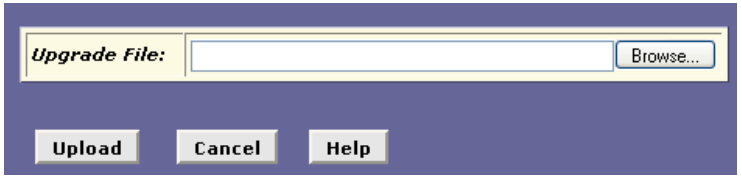
Click on the **Reboot** button after you have made your choice.



10.3 Local Image Upgrade

Click on the **Local Image Upgrade** link to upgrade the software on the modem.
You may easily upgrade the embedded software by obtaining the compressed upgrade kit from the service provider and then following the steps:

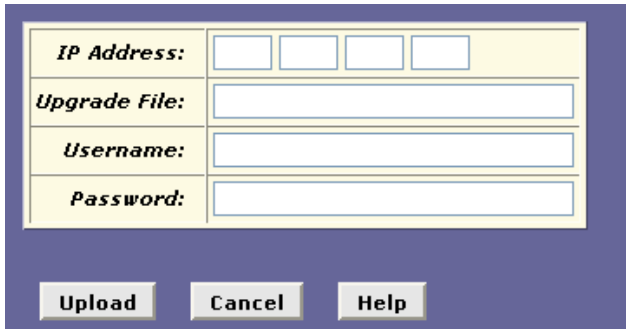
a. Click on the **Browse** button to select the upgrade file.
b. Click on the **Upload** button to upload the file into the modem
c. This process may last as long as 60 seconds.



Note: Strictly maintain stable power to the device while upgrading its software. If the power fails during the upgrading process, contents in the memory could be destroyed, and the system may hang. In such a case, you must call the dealer or system integrator for repairs.

10.4 Remote Image Upgrade

Click on the **Remote Image Upgrade** link to upgrade the software on the modem.
Enter the IP address where the software is located, the name of the software, and the User name and password of the site. Then click on the **Upload** button.

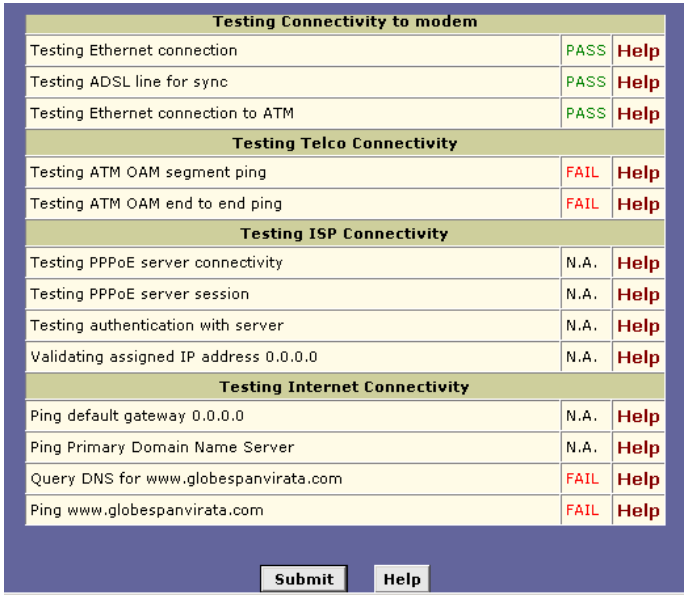


10.5 Alarm

Click on the **Alarm** link to view the list of alarms. The alarms shown in the table have been recorded in response to system events.
Click on the **Clear** button to clear the alarms.

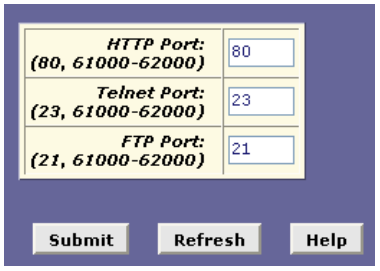
10.6 Diagnostics

Click on the **Diagnostics** link to test the device. Results will be displayed as *pass, fail*, or *N.A,* depending on your settings.
Click on the **Submit** button to begin the diagnostic tests.


Testing Connectivity to modem
Testing Ethernet connection PASS Help
Testing ADSL line for sync PASS Help
Testing Ethernet connection to ATM PASS Help
Testing Telco Connectivity
Testing ATM OAM segment ping FAIL Help
Testing ATM OAM end to end ping FAIL Help
Testing ISP Connectivity
Testing PPPoE server connectivity N.A. Help
Testing PPPoE server session N.A. Help
Testing authentication with server N.A. Help
Validating assigned IP address 0.0.0.0 N.A. Help
Testing Internet Connectivity
Ping default gateway 0.0.0.0 N.A. Help
Ping Primary Domain Name Server N.A. Help
Query DNS for www.globespanvirata.com FAIL Help
Ping www.globespanvirata.com FAIL Help
Submit
Help

10.7 Port Settings

Click on the **Port Settings** link to change the port settings on the device.
Change the settings by entering the new value into the text box and click on the **Submit** button when completed.



10.8 System Log

Click the **System Log** link to display the system logs. The System Log displays data generated or acquired by routine system communication with other devices, such as the results of negotiations with the ISP's computers for DNS and gateway IP addresses. This information does not necessarily represent unexpected or improper functioning and is not captured by the system traps that create alarms.

You can click **Save Log** to display a Windows File Download dialog box that enables opening or saving the contents of the log to your PC. The file is assigned the default name syslog.vlf, and can be viewed with any text editor.

To remove all entries from the list, click **Clear Log**. New entries will begin accumulating and will display when you click **Refresh**.

10.9 Back/ Restore Config

Click on the **Back/Restore Config** link to upload the configuration data from your PC or download it back to the system.
Many of the software features can be configured to address your needs or your ISP's requirements. This configuration data becomes part of the software image. You can extract configuration data from the software image and save it on your PC as a text file. If you later change the system configuration, but then want to revert to the previous settings, you can load the configuration file back to the system.

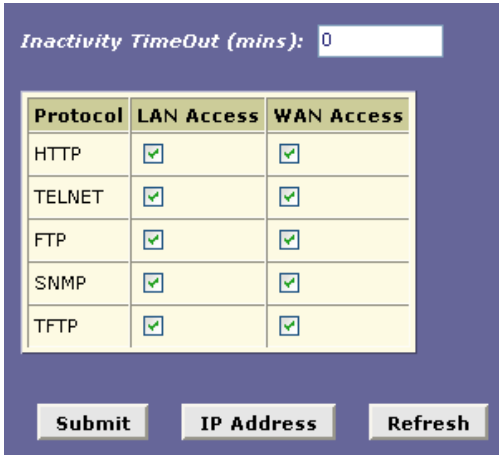
This feature may be especially useful when you receive an image upgrade file from your ISP containing software updates. Uploading the new image may overwrite your customized settings with default values. Before you load the new image, you can store the configuration settings. Then, after you load the image, you can restore your previous configuration.

Click on the **Save Config** button to save the current configuration.
To restore a saved configuration file, click on the **Browse** button and select the file in windows dialog box.
Click on the **Upload** button to restore the selected file from your PC.

10.10 Management control

Click on the **Management control** link to enable access to configuration manager from the WAN port.

The table on this page provides a check box to enable or disable HTTP (i.e., Web browser-based) access to the configuration program through the WAN port. In the **Inactivity TimeOut** text box, you can specify a length of time in minutes after which external access will be blocked, assuming that there is no access during that time.

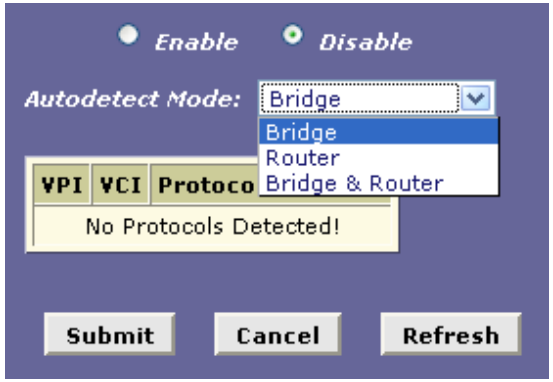


10.11 Autodetect

Click on the **Autodetect** link which enables the modem to automatically detect and configure a valid ATM VC at startup. Autodetect eliminates the need to have users configure VC values.

Autodetect can be used to establish PPPoE, PPPoA, IPoA-1577 and EoA connections and can be configured in either of two modes: **bridging** mode and **routing** mode. These modes are specific to the Autodetect feature and are configured in addition to the system operating mode defined on the modem.

When Autodetect is configured in **bridging** mode, it can detect the presence of PPPoE and EoA interfaces on the access server. In this mode, the modem must be configured as a bridge and a PPPoE or DHCP client is expected to be running on the LAN PC (behind the modem).
When configured in **routing** mode, Autodetect can detect PPPoE, EoA, PPPoA, or IPoA-1577 interfaces on the access server. Autodetect searches for these interfaces in that order. Depending on the interface detected, Autodetect creates a PPP, EoA, or IPoA interface on the modem. In this mode, the modem is expected to be configured as a router.



Click on the **Submit** button when completed and make sure to **Commit & Reboot**.

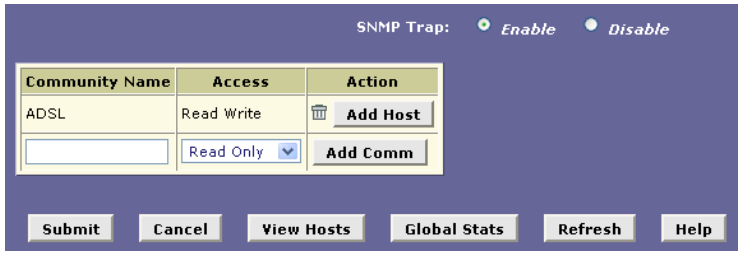
10.12 SNMP

Click on the **SNMP** link to configure the SNMP trap settings. The Simple Network Management Protocol (SNMP) enables a host computer to access configuration, performance, and other system data that resides in a database on the modem. The host computer is called a management station and the modem is called an SNMP agent. The data that can be accessed via SNMP is stored in a Management Information Database (MIB) on the modem.

When SNMP is enabled, the modem responds to SNMP requests from the host. The host may ask to read data from the MIB or, when its privileges allow, write data to it.

Privilege levels are defined by the SNMP communities configured on the modem. A community is a named group of IP addresses. These addresses identify the hosts that are permitted to act as SNMP management stations for accessing the MIB. Each community is defined as having either read-only or read/write privileges.

The data stored in the MIB includes the standard items defined for the SNMP protocol and custom items defined by the ISP. The MIB contents are preconfigured by the ISP and cannot be managed via the Web-based interface.



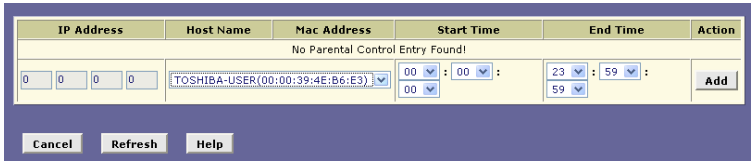
On the SNMP Configuration page, type a **community name** in the empty text box in the left column of the table.
From the **Access** column of the table, select the privileges (read-only or read/write) to assign to all hosts that are part of this community and then click **Add Comm**.

A page displays briefly to confirm your changes, and then the SNMP Configuration page redisplays with the new entry.

Click on the **Submit** button when completed and make sure to **Commit & Reboot**.

10.13 Parental Control

Click on the **Parental Control** link to block Internet access from specified LAN hosts for specified periods.



Ensure that either the system time is specified directly or SNTP is enabled.
In the table on the Parental Control page, enter the IP address of the host you want to block from accessing the Internet.

Select the host name (and corresponding MAC address) from the drop-down list. Host names and MAC addresses will display in the list only when the hosts' IP addresses are distributed from a DHCP server pool configured on the modem (and the host has, in fact, been assigned a host name).

Select the beginning and ending times for the block to be in effect for this host.

Click on the **Add** button to add this entry to the table.

Chapter 3

Quick Protocol Setup

1. Overview

This chapter provides quick steps on setting up the protocols on this device. From this point on, configuration steps are listed for each of the protocols in their respective sections. The seven sections are:

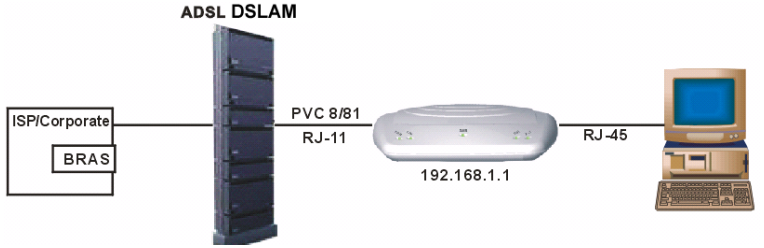
A. RFC 1483 Bridge
B. PPPoE Route Configuration
C. RFC 1483 + NAT
D. PPPoA Route Configuration
E. IPoA Route Configuration
F. DHCP Configuration
G. NAT Configuration

Note: The settings/parameters listed in the next few sections only provide an example to setting up the protocols. Contact your ISP for the actual settings

2. RFC 1483 Bridge

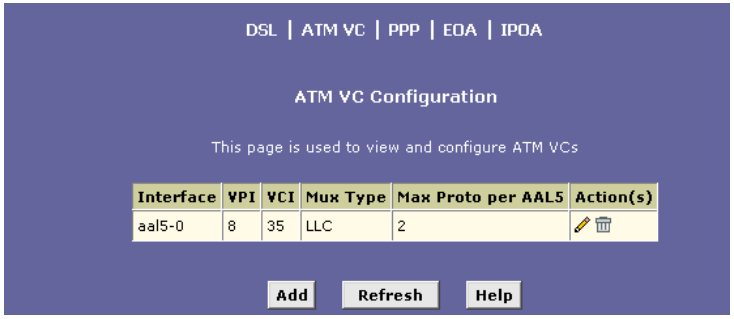
Configuration Table:

Protocol	RFC1483 Bridge Mode.
WAN IP	The ISP assigns the IP address, or have an IP address assigned from an external/internal DHCP server.
Modem IP	192.168.1.1
Gateway IP	None.
VPI/VCI	8/81

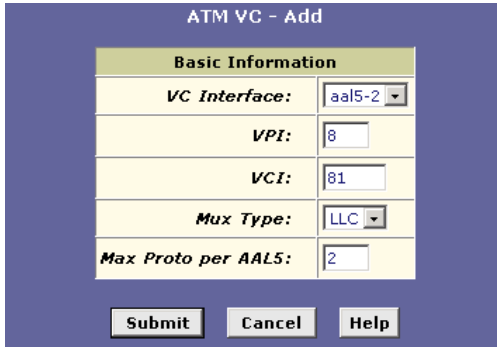


1. Click on the **WAN** tab to view its sub-menu's and configure the WAN settings, then click on the **ATM VC** link below it.

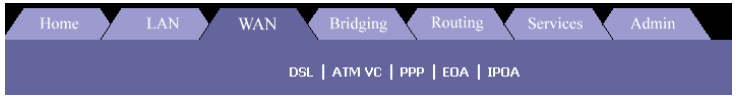
2. You will then see the ATM VC Configuration table. Click on the **Add** button to add a new VPI/VCI setting.



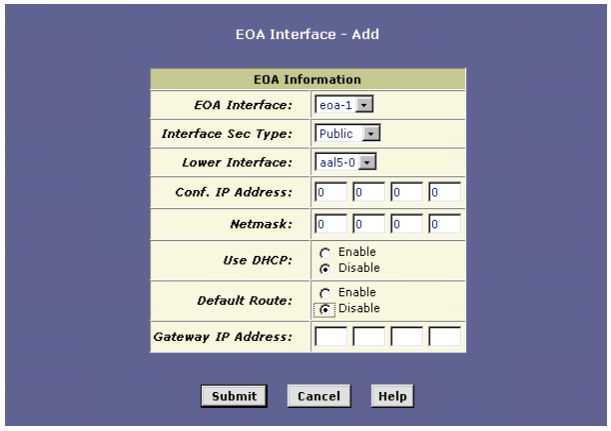
3. Another window will then appear. Enter the VPI/VCI values (8/81) into the VPI and VCI text boxes. Then click on the **Submit** button to confirm the changes.



4. Click on the **EoA** link below the **WAN** tab.

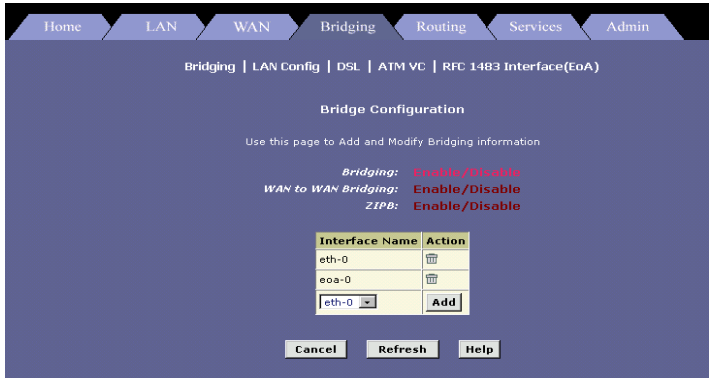


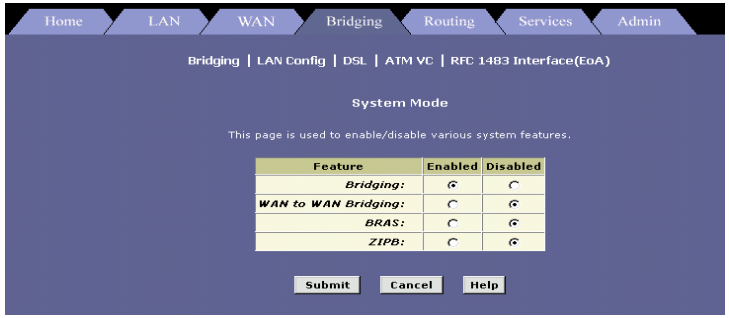
5. Enter the IP address and subnet mask based on your ISP settings. Disable the **Default Route**, because the default gateway is not required in RFC 1483 bridge mode. Then click on the **Submit** button to confirm the changes.



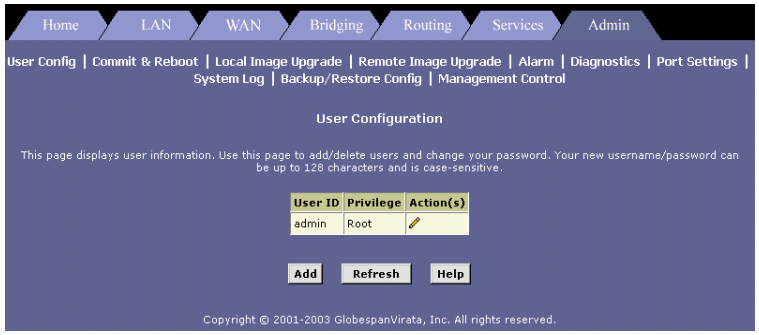
6. Click on the **Bridging** tab to view its sub-menu's and configure the bridging settings, then click on the **Bridging** link below it.

7. Select **EOA-1** from the drop down list, and click on the **Add** button. Then click on the **Submit** button to confirm the changes.

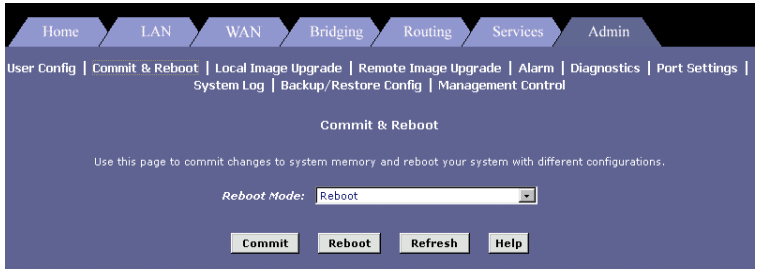




8. Click on the **Admin** tab to view its sub-menu's and configure the bridging settings, then click on the **Commit & Reboot** link below it.


Home
LAN
WAN
Bridging
Routing
Services
Admin
User Config | Commit & Reboot | Local Image Upgrade | Remote Image Upgrade | Alarm | Diagnostics | Port Settings | System Log | Backup/Restore Config | Management Control
User Configuration
This page displays user information. Use this page to add/delete users and change your password. Your new username/password can be up to 128 characters and is case-sensitive.
User ID
Privilege
Action(s)
admin
Root
Add
Refresh
Help
Copyright © 2001-2003 GlobespanVirata, Inc. All rights reserved.

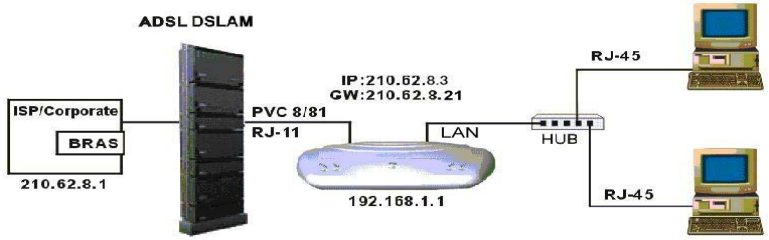
9. Select the **Reboot from last configuration** option from the drop down list, and the click on the **Commit** and **Reboot** button.



3. PPPoE Route Configuration

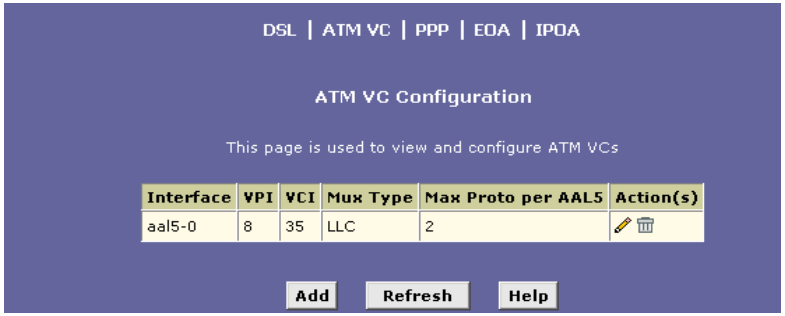
Configuration Table:

Protocol	PPPoE Route Mode + NAT.
LAN IP	192.168.1.xxx or assigned by DHCP server.
Modem IP	192.168.1.1
WAN IP	210.62.8.3
VPI/VC Value	8/81

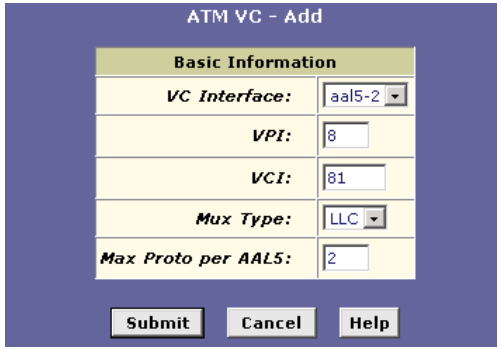


10. Click on the **WAN** tab to view its sub-menu's and configure the WAN settings, then click on the **ATM VC** link below it.

11. You will then see the ATM VC Configuration table. Click on the **Add** button to add a new VPI/VCI setting.

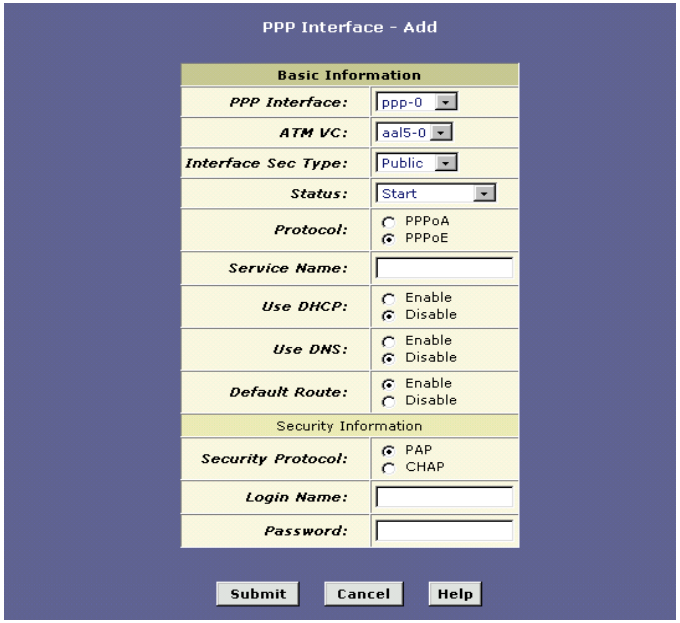


12. Another window will then appear. Enter the VPI/VCI values (8/81) into the VPI and VCI text boxes. Then click on the **Submit** button to confirm the changes.



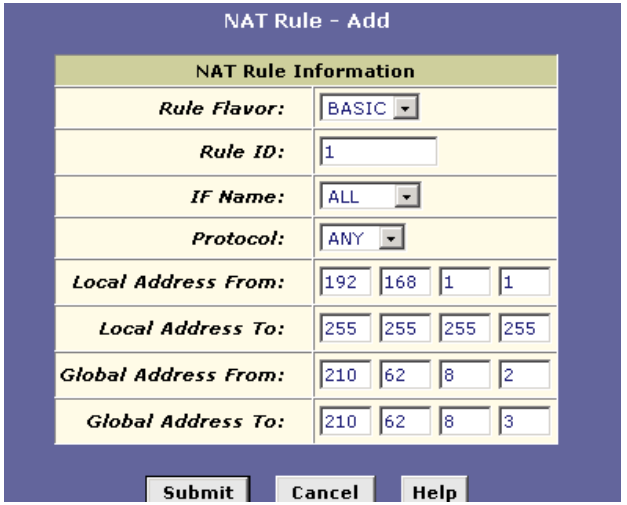
13. Click on the **WAN** tab to view its sub-menu's and configure the WAN settings, then click on the **PPP** link below it.

14. You will then see the PPP Configuration table. Click on the **Add** button to add a new **PPPoE** setting.



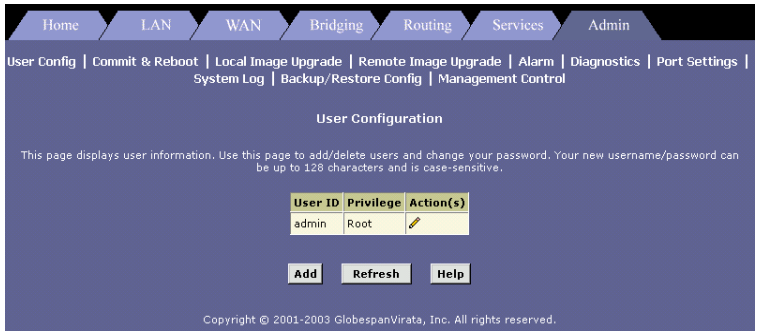
15. Select an interface name: *PPP-1*
16. Select a protocol: *PPPoE*
17. Default Route: *Disable*
18. Security Protocol: Select *PAP* or *CHAP*
19. Login Name: Enter *username* here (from ISP)
20. Password: Enter *password* here (from ISP)
21. Click on the **Submit** button to confirm the changes.
22. Click on the **Services** tab to view its sub-menu's and configure the **NAT** settings, then click on the **NAT** link below it.

23. Select **NAT Rule Entry** from the NAT configuration drop down list. Then click on the **Add** button to add a NAT entry.

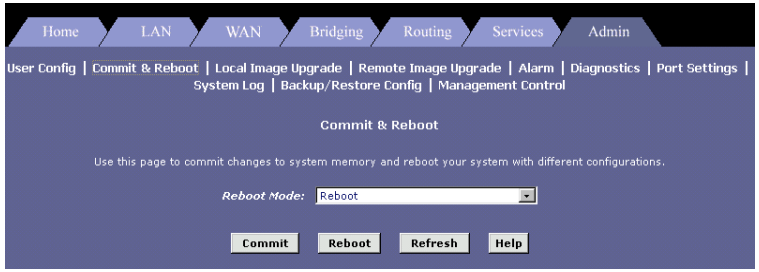


24. Rule Flavor: Select a *Rule flavor* from the drop down list (Basic)
25. Rule ID: *Enter a number here*
26. Local Address From: *Address from where this device will receive IPs*
27. Local Address to: *255.255.255.255 (broadcast) or other*
28. Login Name: Enter *username* here (from ISP)
29. Global Address From: *Global Address from where this device will receive IPs*
30. Global Address From: *Global Address from where this device will send its packets*
31. Click on the **Submit** button to confirm the changes.

32. Click on the **Admin** tab to view its sub-menu's and configure the bridging settings, then click on the **Commit & Reboot** link below it.


Home
LAN
WAN
Bridging
Routing
Services
Admin
User Config | Commit & Reboot | Local Image Upgrade | Remote Image Upgrade | Alarm | Diagnostics | Port Settings | System Log | Backup/Restore Config | Management Control
User Configuration
This page displays user information. Use this page to add/delete users and change your password. Your new username/password can be up to 128 characters and is case-sensitive.
User ID
Privilege
Action(s)
admin
Root
Add
Refresh
Help
Copyright © 2001-2003 GlobespanVirata, Inc. All rights reserved.

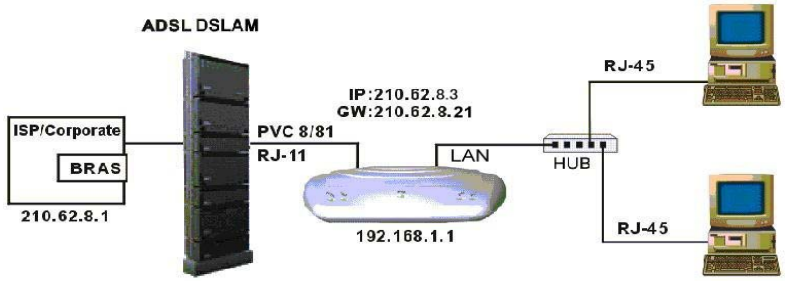
33. Select the **Reboot from last configuration** option from the drop down list, and the click on the **Commit** and **Reboot** button.



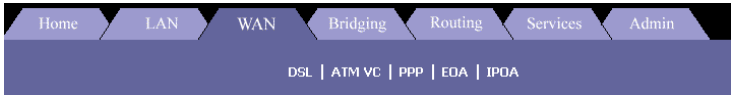
4. RFC 1483 + NAT

Configuration Table:

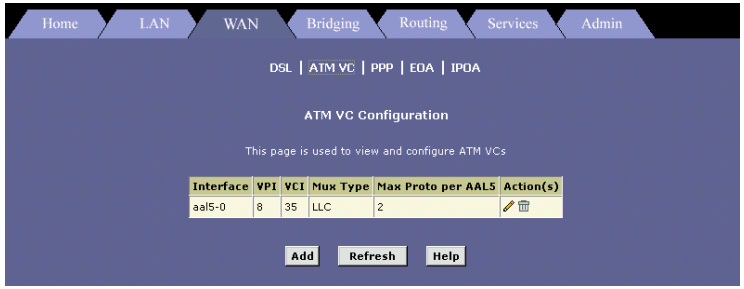
Protocol	RFC1483 Mode + NAT.
LAN IP	192.168.1.xxx or assigned by DHCP server.
Modem IP	192.168.1.1
WAN IP	210.62.8.3
VPI/VC Value	8/81



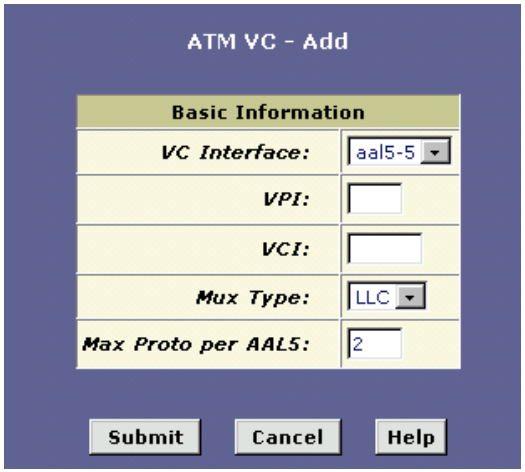
34. Click on the **WAN** tab to view its sub-menu's and configure the WAN settings, then click on the **ATM VC** link below it.



35. You will then see the ATM VC Configuration table. Click on the **Add** button to add a new VPI/VCI setting.



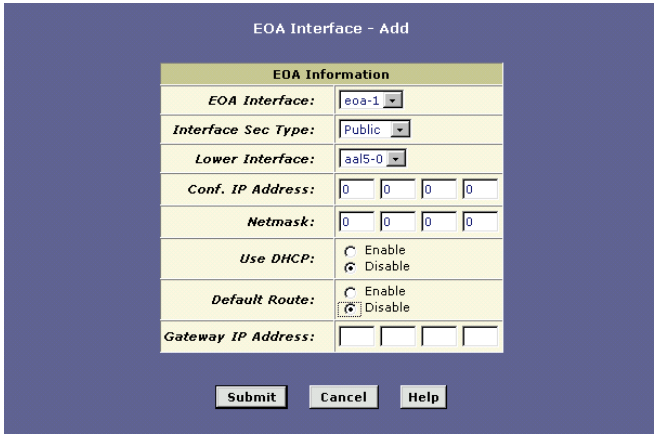
36. Another window will then appear. Enter the VPI/VCI values (8/81) into the VPI and VCI text boxes. Then click on the **Submit** button to confirm the changes.



37. Click on the **EoA** link below the **WAN** tab.

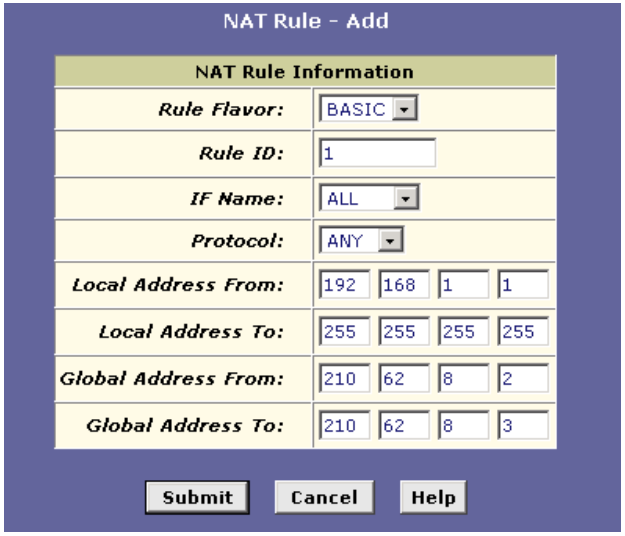
38. Enter the **IP address** and **subnet mask** based on your ISP settings. For example: IP address 210.62.8.3, and subnet mask 255.255.255.0

39. Enable **Default Route** and enter the **Gateway IP Address** (For example, 210.62.8.21), then click on the **Submit** button.

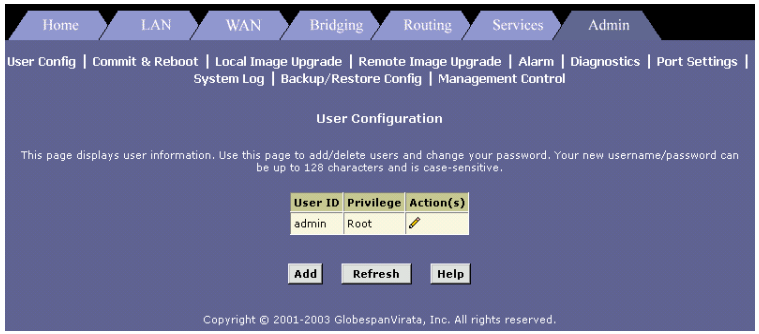


40. Click on the **Services** tab to view its sub-menu's and configure the **NAT** settings, then click on the **NAT** link below it.

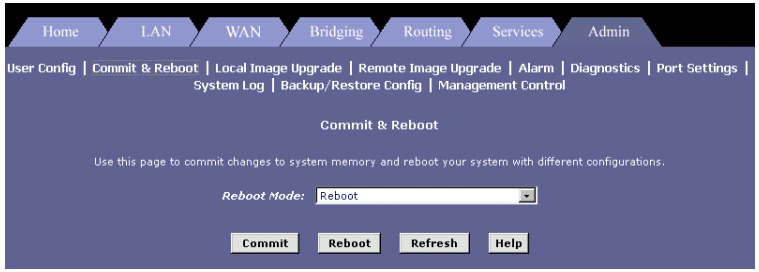
41. Select **NAT Rule Entry** from the NAT configuration drop down list. Then click on the **Add** button to add a NAT entry.



42. Rule Flavor: Select a *Rule flavor* from the drop down list (Basic)
43. Rule ID: *Enter a number here*
44. Local Address From: *Address from where this device will receive IPs*
45. Local Address to: *255.255.255.255 (broadcast) or other*
46. Login Name: Enter *username* here (from ISP)
47. Global Address From: *Global Address from where this device will receive IPs*
48. Global Address From: *Global Address from where this device will send its packets*
49. Click on the **Submit** button to confirm the changes.
50. Click on the **Admin** tab to view its sub-menu's and configure the bridging settings, then click on the **Commit & Reboot** link below it.


Home
LAN
WAN
Bridging
Routing
Services
Admin
User Config | Commit & Reboot | Local Image Upgrade | Remote Image Upgrade | Alarm | Diagnostics | Port Settings | System Log | Backup/Restore Config | Management Control
User Configuration
This page displays user information. Use this page to add/delete users and change your password. Your new username/password can be up to 128 characters and is case-sensitive.
User ID
Privilege
Action(s)
admin
Root
Add
Refresh
Help
Copyright © 2001-2003 GlobespanVirata, Inc. All rights reserved.

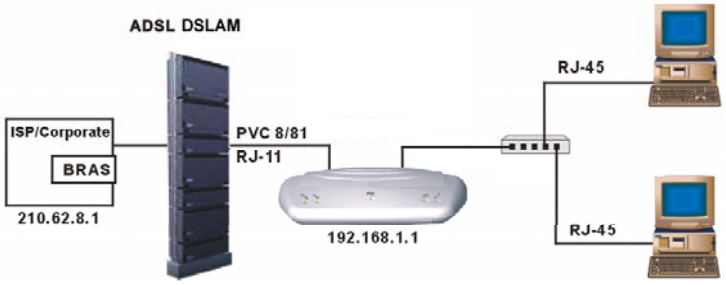
51. Select the **Reboot from last configuration** option from the drop down list, and the click on the **Commit** and **Reboot** button.



5. PPPoA Route Configuration

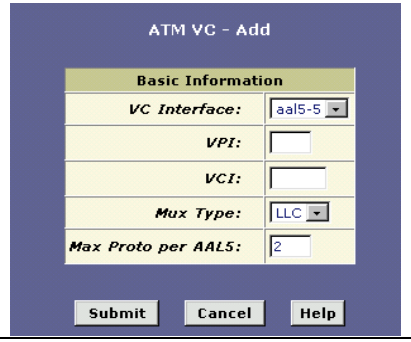
Configuration Table:

Protocol	PPPoA Route Mode.
LAN IP	192.168.1.xxx
Modem IP	192.168.1.1
Gateway IP	Not required.
VPI/VCI	8/81
Username	From ISP.
Password	From ISP.

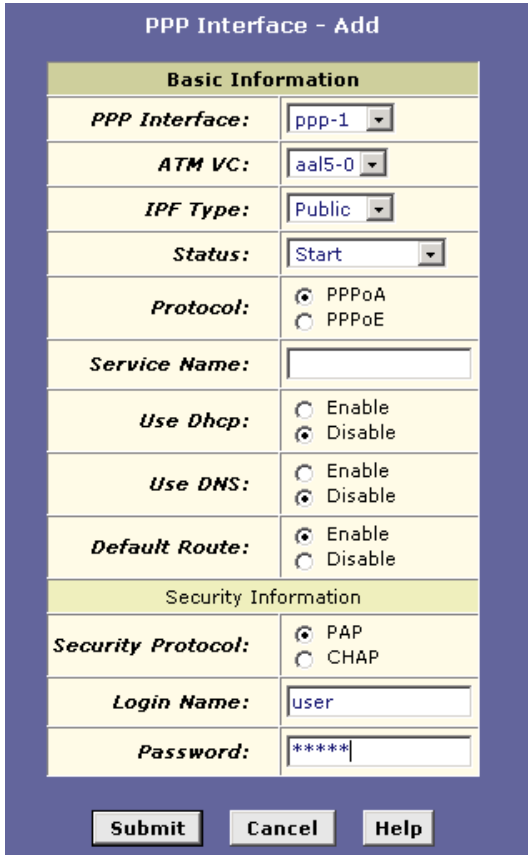


52. Click on the **Routing** tab to view its sub-menu's and configure the Routing settings, then click on the **ATM VC** link below it.

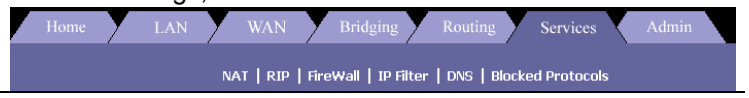
53. You will then see the ATM VC Configuration table. Click on the **Add** button to add a new VPI/VCI setting.
54. Another window will then appear. Enter the VPI/VCI values (8/81) into the VPI and VCI text boxes. Then click on the **Submit** button to confirm the changes.



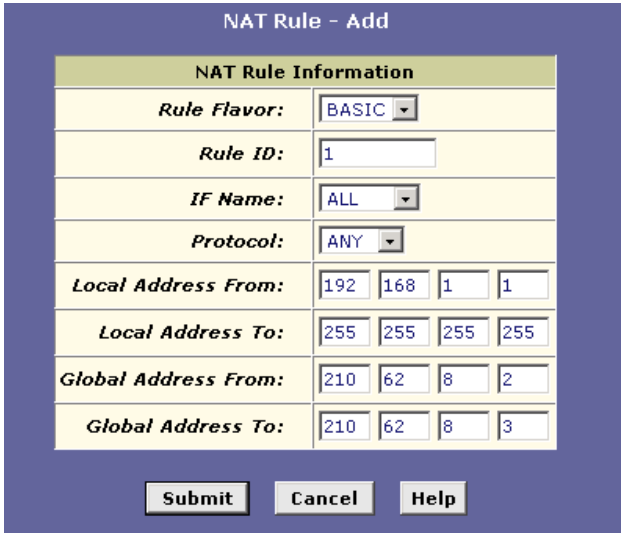
55. Click on the **PPP** link in the **Routing** tab, and then click on the **Add** button to add a **PPPoA** configuration.



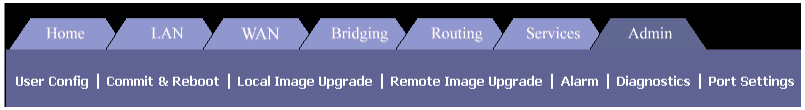
56. Select an interface name: *PPP-1*
57. Select a protocol: *PPPoA*
58. Default Route: *Enable*
59. Security Protocol: Select *PAP* or *CHAP*
60. Login Name: Enter *username* here (from ISP)
61. Password: Enter *password* here (from ISP)
62. Click on the **Submit** button to confirm the changes.
63. Click on the **Services** tab to view its sub-menu's and configure the **NAT** settings, then click on the **NAT** link below it.



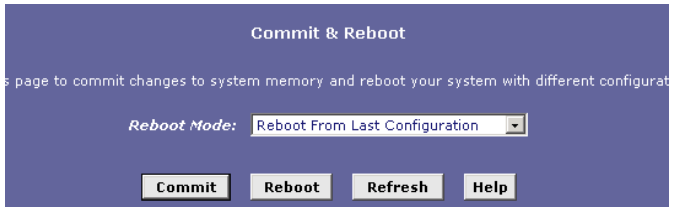
64. Select **NAT Rule Entry** from the NAT configuration drop down list. Then click on the **Add** button to add a NAT entry.



65. Rule Flavor: Select a *Rule flavor* from the drop down list (Basic)
66. Rule ID: *Enter a number here*
67. Local Address From: *Address from where this device will receive IPs*
68. Local Address to: *255.255.255.255 (broadcast) or other*
69. Login Name: Enter *username* here (from ISP)
70. Global Address From: *Global Address from where this device will receive IPs*
71. Global Address From: *Global Address from where this device will send its packets*
72. Click on the **Submit** button to confirm the changes.
73. Click on the **Admin** tab to view its sub-menu's and configure the bridging settings, then click on the **Commit & Reboot** link below it.



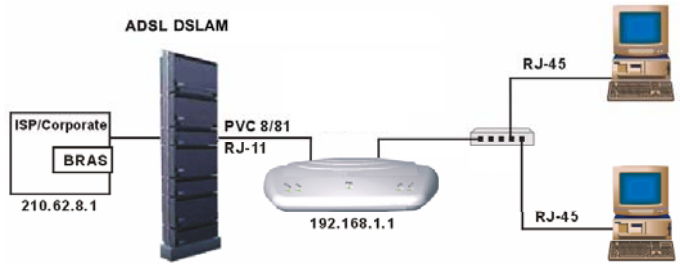
74. Select the **Reboot from last configuration** option from the drop down list, and the click on the **Commit** and **Reboot** button.



6. IPoA Route Configuration

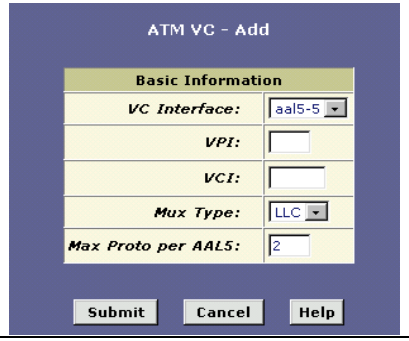
Configuration Table:

Protocol	IPoA Route Mode
LAN IP	192.168.1.xxx
Modem IP	192.168.1.1
Gateway IP	210.62.8.1
VPI/VCI	8/81
WAN IP	210.62.8.2

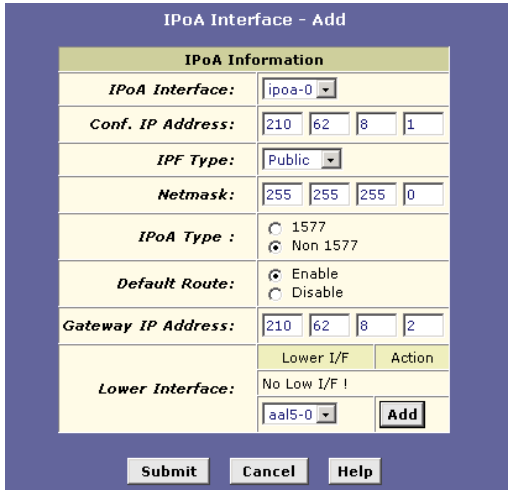


75. Click on the **Routing** tab to view its sub-menu's and configure the Routing settings, then click on the **ATM VC** link below it.

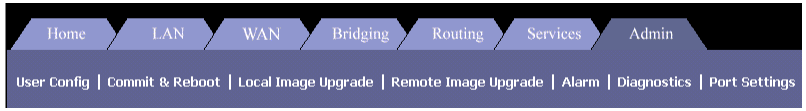
76. You will then see the ATM VC Configuration table. Click on the **Add** button to add a new VPI/VCI setting.
77. Another window will then appear. Enter the VPI/VCI values (8/81) into the VPI and VCI text boxes. Then click on the **Submit** button to confirm the changes.



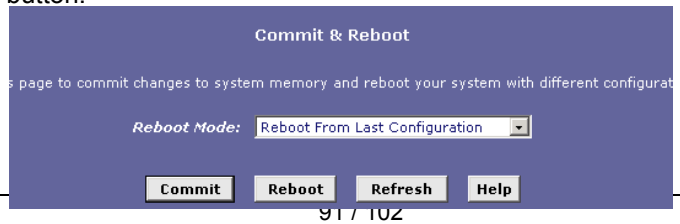
78. Click on the **IPoA** link in the **Routing** tab, and then click on the **Add** button to add an **IPoA** configuration.



79. Select an interface name: *IPoA-0*
80. Conf. IP Address: *From ISP*
81. Net mask: *From ISP*
82. Gateway IP Address: *From ISP*
83. Login Name: Enter *username* here (from ISP)
84. Lower Interface: Select *aal5-0*
85. Click on the **Submit** button to confirm the changes.
86. Click on the **Admin** tab to view its sub-menu's and configure the bridging settings, then click on the **Commit & Reboot** link below it.



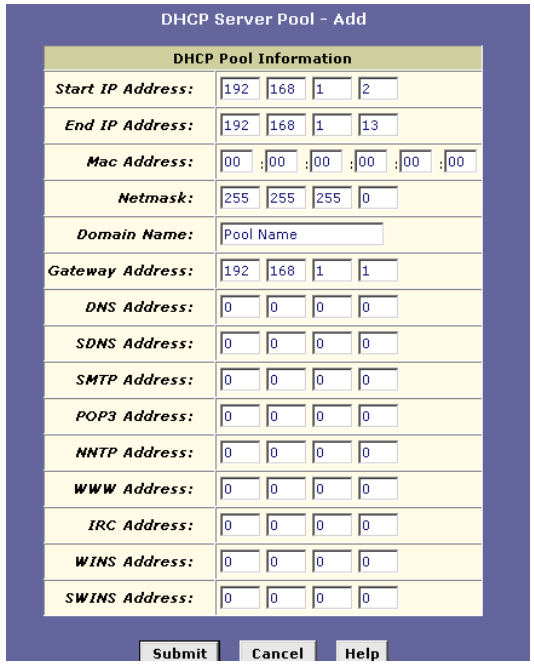
87. Select the **Reboot from last configuration** option from the drop down list, and the click on the **Commit** and **Reboot** button.



7. DHCP Configuration

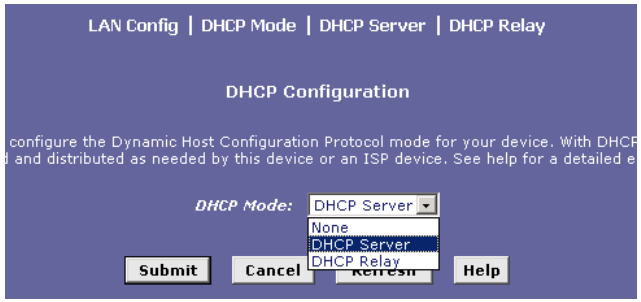
88. Click on the **LAN** tab to view its sub-menu's and configure the **LAN** settings, then click on the **DHCP Mode** link below it.

89. Click on the **DHCP Server** link under the LAN tab, and click on the **Add** button.

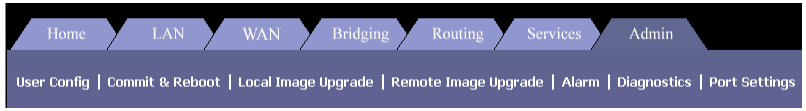


90. Start IP Address: Enter the *Start IP Address (192.168.1.2)*
91. End IP Address: Enter the *End IP Address (192.168.1.13)*
92. Net mask: *based on IP address (255.255.255.0)*
93. Domain Name: Enter a *name* here
94. Gateway IP Address: Enter a Gateway IP Address here
95. Click on the **Submit** button to confirm the changes.

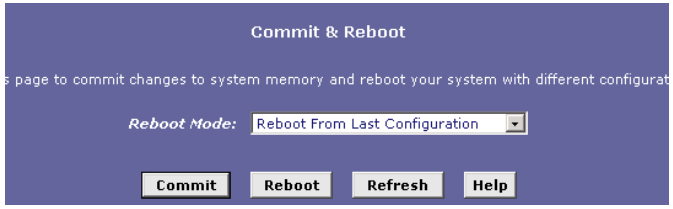
96. From the drop down list, select **DHCP Server**, and click on the **Submit** button.


LAN Config | DHCP Mode | DHCP Server | DHCP Relay
DHCP Configuration
configure the Dynamic Host Configuration Protocol mode for your device. With DHCP
and distributed as needed by this device or an ISP device. See help for a detailed e
DHCP Mode:
DHCP Server
None
DHCP Server
DHCP Relay
Submit
Cancel
Help

97. Click on the **Admin** tab to view its sub-menu's and configure the bridging settings, then click on the **Commit & Reboot** link below it.



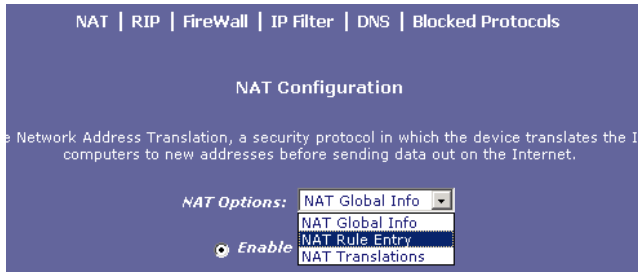
98. Select the **Reboot from last configuration** option from the drop down list, and the click on the **Commit** and **Reboot** button.



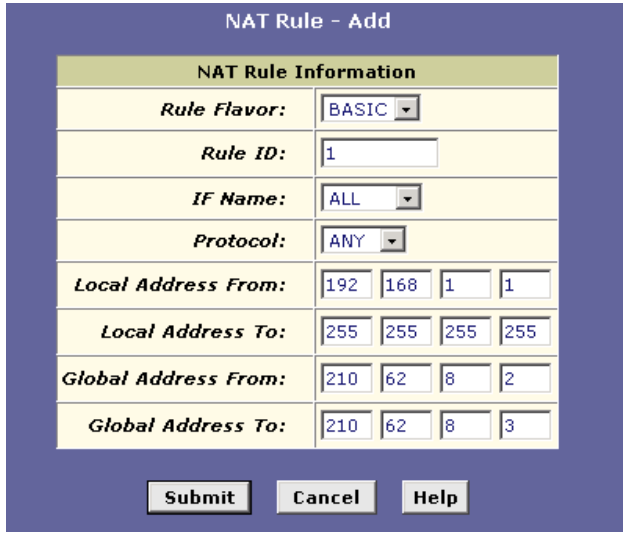
8. NAT Configuration

99. Click on the **Services** tab to view its sub-menu's and configure the **NAT** settings, then click on the **NAT** link below it.

100. From the **NAT Options** drop down list, select **NAT Rule Entry**.


NAT | RIP | FireWall | IP Filter | DNS | Blocked Protocols
NAT Configuration
Network Address Translation, a security protocol in which the device translates the I
computers to new addresses before sending data out on the Internet.
NAT Options:
NAT Global Info
NAT Global Info
NAT Rule Entry
NAT Translations
Enable

101. Click on the **Add** button to add a new **NAT Rule Entry**.



102. Rule Flavor: Select a *Rule flavor* from the drop down list (Basic)
103. Rule ID: *Enter a number here*
104. Local Address From: *Address from where this device will receive IPs*
105. Local Address to: *255.255.255.255 (broadcast) or other*
106. Login Name: Enter *username* here (from ISP)
107. Global Address From: *Global Address from where this device will receive IPs*
108. Global Address From: *Global Address from where this device will send its packets*
109. Click on the **Submit** button to confirm the changes.

Appendix A – Specifications

A1. Hardware Specifications

- **LAN Interface**
  - One 10/100 Base-TX Ethernet port, IEEE 802.3/3u, RJ-45 connector
  - One USB 1.1 device port, type B connector
- **WAN Interface (ADSL line)**
  - One pair (2-wire) loop, 100 Ω line impedance with RJ-11 connector
  - Compliance of X8824r: ITU-T G.992.1, G.992.2 and ANSI T1.413 Issue 2
  - Compliance of X8824r+: ITU-T G.992.1, G.992.2, G.992.3, G.992.5 and ANSI T1.413 Issue 2
- **Indicators**
  - **USB** (green LED) – Continuous ON when USB link is active; blinking while transmitting / receiving data
  - **LAN** (green LED) – Continuous ON when Ethernet is active; blinking while transmitting / receiving data
  - **PPP** (green LED) – Continuous ON when PPP connection is established; blinking while transmitting / receiving data
  - **WAN** (green LED) – Continuous ON when ADSL link is up
  - **PWR** (green LED) – Continuous ON when power is properly connected
- **OAM&P**
  - Local: Telnet or Web management via Ethernet
  - Remote: Telnet or Web Management
- **Power**
  - AC adapter: Input 110/220VAC, 50/60Hz; Output 15VAC 1A
  - Power consumption: Less than 6 Watts
- **Environment**
  - Operation Temperature and Humidity: 0°C ~ 45°C, 5% ~ 95% (non-condensing)
  - Storage Temperature and Humidity: -20°C ~ 85°C, 5% ~ 95% (non-condensing)
- **Physical Dimensions**
  - (W × D × H) 160 mm × 115 mm × 35 mm
- **Certificates**
  - CE, CB

A2. Software Specifications

- **ATM**
  - ATM cells over ADSL, AAL5
  - Supports 8 PVCs under bridge mode and 5 PVCs under router mode
  - Supports UBR, CBR, rt-VBR, nrt-VBR and GFR traffic classes
  - ADSL-aware CAC (Connection Admission Control)
  - Support for F5 AIS, RDI, and loopback cells
  - Payload encapsulation
    - RFC2684 / RFC1483, Multiprotocol Encapsulation over ATM Adaptation Layer 5
    - RFC2225 / RFC1577, Classical IP and ARP over ATM (IPoA)
    - RFC2364, PPP over AAL5 (PPPoA)
- **Bridging**
  - RFC2684 / RFC1483 bridged PDU encapsulation
  - IEEE 802.1D transparent bridging and spanning tree protocol
  - ZIPB (Zero Installation PPP Bridge)
- **Routing**
  - RFC2684 / RFC1483 routed PDU encapsulation
  - Supports Point-to-Point Protocol (including PPPoA and PPPoE) and user authentication via PAP or CHAP
  - Supports TCP, UDP, ARP, RARP, IPCP, ICMP, IGMP, etc.
  - IP routing: static route, RIP v1 and v2
  - NAT/PAT with extensive ALG supports
  - DNS relay agent
  - Layer 2 tunneling protocol (L2TP)
- **Security**
  - Built-in firewall with protection against DOS attacks, IP spoofing, and other common types of attacks
  - Packet filtering at MAC layer (raw filter) and IP layer, including stateful packet filtering
  - Supports blacklist
- **Configuration and Network Management**
  - TR037-compliant auto-configuration using ILMI
  - SNMP v1 agent – over IP, ILMI VCC or HDLC/EOC
  - DHCP client, server and relay for IP management
  - Universal Plug and Play (UPnP) support
  - Telnet with CLI (command line interface) or Web-based configuration and management
  - FTP/TFTP or HTTP for firmware upgrade and configuration
- **USB drivers for host PC / MAC**
  - Driver support for Microsoft Windows 98, 98SE, ME, 2000, XP, Linux, MAC OS 8, 9 and X

Appendix B – Warranties

B1. Product Warranty

1. XAVi Technologies warrants that the ADSL unit will be free from defects in material and workmanship for a period of twelve (12) months from the date of shipment.
2. XAVi Technologies shall incur no liability under this warranty if
   - The allegedly defective goods are not returned prepaid to XAVi Technologies within thirty (30) days of the discovery of the alleged defect and in accordance with XAVi Technologies' repair procedures; or
   - XAVi Technologies' tests disclose that the alleged defect is not due to defects in material or workmanship.
3. XAVi Technologies' liability shall be limited to either repair or replacement of the defective goods, at XAVi Technologies' option.
4. XAVi Technologies MARKS NO EXPRESS OR IMPLIED WARRANTIES REGARDING THE QUALITY, MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE BEYOND THOSE THAT APPEAR IN THE APPLICABLE USER'S DOCUMETATION. XAVi SHALL NOT BE RESPONSIBLE FOR CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGE, INCLUDING, BUT NOT LIMITED TO, LOSS OF PROFITS OR DAMAGES TO BUSINESS OR BUSINESS RELATIONS. THIS WARRANTY IS IN LIEU OF ALL OTHER WARRANTIES.

B2. Warranty Repair

1. During the first three (3) months of ownership, XAVi Technologies will repair or replace a defective product covered under warranty within twenty-four (24) hours of receipt of the product. During the fourth (4th) through twelfth (12th) months of ownership, XAVi Technologies will repair or replace a defective product covered under warranty within ten (10) days of receipt of the product. The warranty period for the replaced products shall be ninety (90) days or the remainder of the warranty period of the original unit, whichever is greater. XAVi Technologies will ship surface freight. Expedited freight is at customer's expense.
2. The customer must return the defective product to XAVi Technologies within fourteen (14) days after the request for replacement. If the defective product is not returned within this time period, XAVi Technologies will bill the customer for the product at list price.

B3. Out-of-Warranty Repair

XAVi Technologies will either repair or, at its option, replace a defective product not covered under warranty within ten (10) working days of its receipt. Repair charges are available from the Repair Facility upon request. The warranty on a serviced product is thirty (30) days measured from date of service. Out-of-warranty repair charges are based upon the prices in effect at the time of return.

Appendix C – Regulations

C1. FCC Part 15 Notice

Warning: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 to the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a residential environment. This equipment generates, used, and can radiate radio frequency energy, and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is unlikely to cause harmful interference. But if it does, the user will be required to correct the interference at his or her own expense. The authority to operate this equipment is conditioned by the requirement that no modifications will be made to the equipment unless XAVi expressly approves the changes or modifications.

C2. IC CS-03 Notice

The Industry Canada label identifies certified equipment. This certification means that the equipment meets certain telecommunications network protective, operational, and safety requirements as prescribed in appropriate Terminal Equipment Technical Requirements document(s). The Department does not guarantee that the equipment will operate to the user's satisfaction.

Before installing this equipment, users should make sure that it is permissible to be connected to the facilities of the local telecommunications company. An acceptable method of connection must be used to install the equipment. The customer should be aware that compliance with the above conditions might not prevent degradation of service in some situations.

Repairs to certified equipment should be coordinated by a representative designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines, and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

Warning: Users should not attempt to make such connections themselves, but should contact appropriate electric inspection authority, or electrician, as appropriate.

Contact Information

You can help us serve you better by sending us your comments and feedback. Listed below are the addresses, telephone and fax numbers of our offices. You can also visit us on the World Wide Web at www.xavi.com.tw for more information. We look forward to hearing from you!

WORLD HEADQUARTER
XAVi Technologies Corporation
9F, No. 129 Hsing Te Road, Sanchung City
Taipei County 241, Taiwan
Tel: +886-2-2995-7953 Fax: +886-2-2995-7954

USA BRANCH OFFICE
53 Parker
Irvine, CA 92618
Tel: +1-949-380-7550 Fax: +1-949-380-9204

28 Vista Drive
Morganville, NJ 07751
Tel: +1-732-972-9363 Fax: +1-732-972-9271

S.AMERICA OFFICE
Tel: +55 -11-4485-3143

EUROPEAN BRANCH OFFICE
Oehleckerring 6B, 22419 Hamburg, Germany
Tel: +49-40-514400-53 Fax: +49-40-514400-79

5, Place de la Pyramide
Tour Ariane, La Defense 9
92088 Paris-La Defense Cedex
France
Tel 1: +33-1-55-68-11-08 Fax: +33-1-55-68-10-00
Tel 2: +33-1-55-68-11-09

CHINA SUBSIDIARY
Room 401, Floor 4, #608 ZhaoJiaBang Road,
Shanghai, 200031
Tel: +86-21-6431-8800 Fax: +86-21-6431-7885